

5. WYKŁAD 5: KONSTRUKCJA CIAŁ p^n -ELEMENTOWYCH.

Definicja 5.1. Niech $(R, +, \cdot)$ będzie pierścieniem. Podzbiór $I \subset R$ nazywamy **ideałem** pierścienia R , co oznaczamy przez $I \triangleleft R$, jeżeli:

- (1) $\forall a, b \in I (a - b \in I)$,
- (2) $\forall a \in I \forall r \in R (ra \in I)$.

Przykład:

- (1) Zbiór $\{n : 5|n\}$ jest ideałem w pierścieniu $\mathbb{Z}$.
- (2) Zbiór $\{f : x|f\}$ jest ideałem w pierścieniu $\mathbb{R}[x]$.

Definicja 5.2. Niech $(R, +, \cdot)$ będzie pierścieniem, a $A \subset R$ pewnym zbiorem. Najmniejszy ideał pierścienia R zawierający zbiór A nazywamy **ideałem generowanym przez A** i oznaczamy (A) . Jeśli $I \triangleleft R$, to każdy zbiór A o tej własności, że $(A) = I$ nazywamy **zbiorem generatorów ideału I** . Jeśli $A = \{a_1, \dots, a_n\}$, to piszemy po prostu

$$(a_1, \dots, a_n) = (A).$$

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

$$I = (a_1, \dots, a_n).$$

Mówimy, że ideał jest **główny**, gdy istnieje element $a \in R$ taki, że

$$I = (a).$$

Mówimy, że pierścień R jest **pierścieniem ideałów głównych**, gdy każdy jego ideał jest ideałem głównym.

Twierdzenie 5.3 (o postaci elementów ideału generowanego przez zbiór). Niech $(R, +, \cdot)$ będzie pierścieniem, a $A \subset R$ pewnym zbiorem. Wówczas:

$$(A) = \{r_1 a_1 + \dots + r_n a_n : n \in \mathbb{N}, r_1, \dots, r_n \in R, a_1, \dots, a_n \in A\}.$$

Dowód. Oznaczmy:

$$A_1 = \{r_1 a_1 + \dots + r_n a_n : n \in \mathbb{N}, r_1, \dots, r_n \in R, a_1, \dots, a_n \in A\}.$$

Pokażemy, że $A_1 \triangleleft R$. Istotnie, jeśli $r_1 a_1 + \dots + r_n a_n, r'_1 a'_1 + \dots + r'_m a'_m \in A_1$, to $r_1 a_1 + \dots + r_n a_n + (-r'_1) a'_1 + \dots + (-r'_m) a'_m \in A_1$. Ponadto dla $r \in R$ mamy $r(r_1 a_1 + \dots + r_n a_n) = rr_1 a_1 + \dots + rr_n a_n \in A_1$.

Dalej, pokażemy, że $A_1 = (A)$. Inkluzja $(\supset)$ jest oczywista, pozostaje wykazać $(\subset)$. Dowód prowadzimy przez indukcję względem n . Dla $n = 1$ niech $a_1 \in A$. Wówczas $r_1 a_1$ należy do każdego ideału zawierającego a , w szczególności do (A) . Dla $n > 1$ ustalmy $a_1, \dots, a_n \in A, r_1, \dots, r_n \in R$ i założmy, że

$$r_1 a_1 + \dots + r_n a_n \in (A).$$

Ustalmy $a_{n+1} \in A$ oraz $r_{n+1} \in R$. Wówczas

$$\underbrace{r_1 a_1 + \dots + r_n a_n}_{\in (A)} + \underbrace{r_{n+1} a_{n+1}}_{\in (A)} \in (A).$$

□

Przykłady:

(3) W pierścieniu $\mathbb{Z}$ mamy na przykład

$$(5) = \{k \cdot 5 : k \in \mathbb{Z}\}$$

oraz

$$(4, 6) = \{k \cdot 4 + l \cdot 6 : k, l \in \mathbb{Z}\}.$$

(4) W pierścieniu $\mathbb{R}[x]$ mamy

$$(x) = \{f \cdot x : f \in \mathbb{R}[x]\}.$$

Twierdzenie 5.4. *Niech $(F, +, \cdot)$ będzie ciałem. Wówczas pierścień wielomianów $(F[x], +, \cdot)$ jest pierścieniem ideałów głównych.*

Dowód. Ustalmy ideał $I \triangleleft F[x]$. Jeśli $I = \{0\}$, to $I = (0)$ jest ideałem głównym. Jeśli $I \neq \{0\}$, to istnieje niezerowy element $f \in I$. W szczególności zbiór

$$H = \{f \in I : f \text{ jest możliwie najniższego stopnia oraz } f \neq 0\}$$

jest niepusty. Ustalmy $h \in H$.

Pokażemy, że $I = (h)$. Inkluzja $(\supset)$ jest oczywista, pozostaje wykazać $(\subset)$. Ustalmy $g \in I$. Dzieląc z resztą g przez h otrzymujemy

$$g = qh + r \text{ dla } q, r \in F[x], 0 \leq \deg(r) < \deg(h).$$

W szczególności $r = g - qh \in I$. Skoro $\deg(r) < \deg(h)$, więc wobec wyboru wielomianu h otrzymujemy, że $r = 0$. Zatem $g = qh$ i tym samym $g \in (h)$. $\square$

Definicja 5.5. *Niech $(R, +, \cdot)$ będzie pierścieniem, a $I \triangleleft R$ ideałem. Warstwą elementu $a \in R$ względem ideału I nazywamy zbiór*

$$a + I = \{a + i : i \in I\}.$$

Zbiór wszystkich warstw oznaczamy przez R/I .

Przykłady:

(5) W pierścieniu $\mathbb{Z}_6$ ideał główny generowany przez element $2 \in \mathbb{Z}_6$ ma postać:

$$(2) = \{0, 2, 4\}.$$

Warstwy tego ideału to:

$$\begin{aligned} 0 + (2) &= \{0 + 0, 0 + 2, 0 + 4\} = (2), \\ 1 + (2) &= \{1, 3, 5\} = W, \\ 2 + (2) &= \{0, 2, 4\} = (2), \\ 3 + (2) &= \{1, 3, 5\} = W, \\ 4 + (2) &= (2), \\ 5 + (2) &= W. \end{aligned}$$

Zatem $\mathbb{Z}_6/(2) = \{(2), W\}$.

(6) W pierścieniu $\mathbb{Z}$ ideał główny generowany przez element $3 \in \mathbb{Z}$ ma postać:

$$(3) = \{0, 3, 6, 9, \dots, -3, -6, -9, \dots\}.$$

Warstwy tego ideału to

$$\begin{aligned} 0 + (3) &= (3), \\ 1 + (3) &= \{1, 4, 7, 10, \dots, -2, -5, -8, \dots\} = W_1, \\ 2 + (3) &= \{2, 5, 8, 11, \dots, -1, -4, -7, \dots\} = W_2, \\ 3 + (3) &= (3). \end{aligned}$$

Zatem $\mathbb{Z}/(3) = \{(3), W_1, W_2\}$. Zauważmy ponadto, że warstwa W_1 składa się z tych liczb całkowitych, które przy dzieleniu przez 3 dają resztę 1, a warstwa W_2 składa się z tych liczb całkowitych, które przy dzieleniu przez 3 dają resztę 2. Tym samym $\mathbb{Z}/(3)$ można utożsamić z $\mathbb{Z}_3$.

- (7) Kluczowa konstrukcja tego wykładu to przeniesienie pomysłu z przykładu (6) na pierścień wielomianów nad ciałem skończonym.

W pierścieniu $\mathbb{Z}_2[x]$ ideał główny generowany przez wielomian $x^2 + x + 1$ ma postać

$$(x^2 + x + 1) = \{x^2 + x + 1, x^3 + x^2 + x, x^3 + x^2 + x + x^2 + x + 1, \dots, f \cdot (x^2 + x + 1)\}.$$

Przykładowe warstwy tego ideału to:

$$\begin{aligned} 0 + (x^2 + x + 1) &= (x^2 + x + 1), \\ 1 + (x^2 + x + 1) &= W_1, \\ x + (x^2 + x + 1) &= W_2, \\ x + 1 + (x^2 + x + 1) &= W_3. \end{aligned}$$

Pokażemy, że dowolna inna warstwa tego ideału będzie równa $(x^2 + x + 1)$, W_1 , W_2 lub W_3 . Istotnie, ustalmy warstwę $f + (x^2 + x + 1)$ i niech $g \in f + (x^2 + x + 1)$. Wówczas $g = f + q(x^2 + x + 1)$. Dzieląc f z resztą przez $x^2 + x + 1$ otrzymujemy:

$$f = q_1(x^2 + x + 1) + r_1 \text{ oraz } 0 \leq \deg(r_1) < \deg(x^2 + x + 1) = 2.$$

Jedyne możliwe wybory dla r_1 to:

$$0, 1, x, x + 1$$

a zatem jeżeli, na przykład, $r_1 = x + 1$, to wówczas:

$$\begin{aligned} g &= f + q(x^2 + x + 1) = q_1(x^2 + x + 1) + (x + 1) + q(x^2 + x + 1) \\ &= (x + 1) + (q_1 + q)(x^2 + x + 1) \in W_3. \end{aligned}$$

Zatem $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{(x^2 + x + 1), W_1, W_2, W_3\}$ i zbiór warstw $\mathbb{Z}_2[x]/(x^2 + x + 1)$ można utożsamiać z możliwymi resztami z dzielenia przez wielomian $x^2 + x + 1$.

Twierdzenie 5.6. Niech $(F, +, \cdot)$ będzie ciałem, niech $p \in F[x]$ będzie wielomianem nierozkładalnym, to znaczy takim, że jeśli

$$p = f \cdot g, \text{ dla } f, g \in F[x],$$

to $\deg(f) = 0$ lub $\deg(g) = 0$. W zbiorze warstw $F[x]/(p)$ definiujemy dodawanie

$$(f + (p)) + (g + (p)) = (f + g) + (p)$$

oraz mnożenie

$$(f + (p)) \cdot (g + (p)) = (f \cdot g) + (p).$$

Wówczas $(F[x]/(p), +, \cdot)$ jest ciałem.

Dowód. Pokażemy, dla przykładu, że dowolny element $\neq (p)$ jest odwracalny. Ustalmy $f + (p) \in F[x]/(p)$. Ponieważ $f + (p) \neq (p)$, więc $f \notin (p)$ i tym samym $p \nmid f$. Ponadto p jest nierozkładalny, a więc $NWD(f, p) = 1$. Wobec algorytmu Euklidesa istnieją $a, b \in F[x]$ takie, że

$$af + bp = 1.$$

Wówczas $af = 1 - bp \in 1 + (p)$, a więc $(a + (p)) \cdot (f + (p)) = 1 + (p)$. □

Uwaga 5.7. Niech $(F[x]/(p), +, \cdot)$ będzie ciałem zdefiniowanym przez wielomian nierozkładalny $p \in F[x]$, gdzie $\deg(p) = n + 1$. Przyjmujemy oznaczenie:

$$a_n a_{n-1} \dots a_1 a_0 = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 + (p).$$

Przykład:

(8) Zgodnie z powyższą notacją:

$$10 = x + (x^2 + x + 1)$$

w ciele $\mathbb{Z}_2[x]/(x^2 + x + 1)$.