

Pierścień wielomianów

Definicja:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem.

1. Element $x \in R$ taki, że

$$\exists y \in R \setminus \{0\} (x \cdot y = 0)$$

nazywamy **dzielnikiem zera**. Zbiór wszystkich dzielników zera oznaczamy $\mathcal{D}(R)$.

2. Element $x \in R$ taki, który nie jest dzielnikiem zera, nazywamy **elementem regularnym**.

Przykłady:

1. Rozważmy dowolny pierścień $(R, +, \cdot)$. Element 0 jest zawsze dzielnikiem zera, nazywamy go **niewłaściwym** dzielnikiem zera. Każdy inny dzielnik nazywać będziemy **właściwym** dzielnikiem zera.
2. Rozważmy pierścień $\mathbb{Z}_6$. Wówczas elementy 0, 2, 3, 4 są dzielnikami zera, a elementy 1, 5 są regularne.
3. Rozważmy pierścień $\mathbb{Z} \times \mathbb{Z}$. Wówczas elementy $(1, 0)$ i $(0, 1)$ są dzielnikami zera.

Twierdzenie:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, niech $x, y, z \in R$.
Wówczas:

1. $x \cdot y = 0 \Rightarrow x \in \mathcal{D}(R) \vee y \in \mathcal{D}(R)$;
2. jeśli x jest regularny, to

$$x \cdot y = 0 \Rightarrow x = 0;$$

3. jeśli x jest regularny, to

$$x \cdot y = x \cdot z \Rightarrow y = z.$$

Przykład:

4. Rozważmy pierścień $\mathbb{Z}_6$. Wówczas $3 \cdot 2 = 3 \cdot 4$, ale $2 \neq 4$.

Definicja:

Pierścień bez właściwych dzielników zera nazywamy **pierścieniem całkowitym** (lub **dziedziną całkowitości**).

Przykład:

5. Przykładami pierścieni całkowitych są $\mathbb{Z}$, $\mathbb{Z}_5$, czy ogólnie $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą.

Uwaga i definicja:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem.

Wielomianem zmiennej x o współczynnikach w pierścieniu R będziemy nazywali wyrażenie o postaci

$$a_0 + a_1x + \dots + a_nx^n,$$

gdzie $n \in \mathbb{N}$ oraz $a_0, \dots, a_n \in R$.

Dwa wielomiany uważamy za **równe** wtedy i tylko wtedy, gdy różnią się tylko o składniki postaci $0 \cdot x^i$, gdzie $i \in \mathbb{N}$.

Będziemy mówili, że wielomian $f = a_0 + a_1x + \dots + a_nx^n$ jest **stopnia** n , gdy $a_n \neq 0$.

Umowa ta nie określa stopnia wielomianu 0, przyjmujemy więc dodatkowo, że stopniem wielomianu 0 jest $-\infty$.

Stopień wielomianu f będziemy oznaczać przez $\deg(f)$.

Wielomiany stopnia 1 będziemy nazywać **liniowymi**, a wielomiany stopnia 2 **kwadratowymi**.

Dla wielomianu $f = a_0 + a_1x + \dots + a_nx^n$ współczynnik a_n nazywamy **najstarszym** (lub **największym**) współczynnikiem. Jeżeli najstarszy współczynnik równy jest 1, to wielomian f nazywamy **unormowanym**.

W zbiorze wszystkich wielomianów zmiennej x o współczynnikach z pierścienia R definiujemy dodawania $+$ i mnożenie $\cdot$, kładąc dla dowolnych wielomianów $f = a_0 + a_1x + \dots + a_nx^n$ oraz $g = b_0 + b_1x + \dots + b_mx^m$

$$f + g = \begin{cases} (a_0 + b_0) + (a_1 + b_1)x + (a_n + b_n)x^n \\ \quad + b_{n+1}x^{n+1} + \dots + b_mx^m, & \text{gdy } m > n, \\ (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n, & \text{gdy } m = n, \\ (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m \\ \quad + a_{m+1}x^{m+1} + \dots + a_nx^n, & \text{gdy } m < n, \end{cases}$$

$$f \cdot g = c_0 + c_1x + \dots + c_{n+m}x^{n+m},$$

gdzie

$$c_i = \sum_{k=0}^i a_{i-k} b_k,$$

dla $i \in \{0, \dots, n + m\}$.

Ponadto wyróżniamy wielomian 0 jako element neutralny dodawania oraz wielomian 1 jako element neutralny mnożenia. Wówczas zbiór wszystkich wielomianów zmiennej x o współczynnikach z pierścienia R z tak określonymi działaniami i wyróżnionymi elementami jest pierścieniem przemennym z jedyneką. Pierścień ten będziemy nazywali **pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R** i będziemy oznaczali przez $R[x]$.

Uwaga:

Przy liczeniu stopni wielomianów przyjmujemy następującą umowę notacyjną:

- ▶ $\forall n \in \mathbb{N}(n > -\infty),$
- ▶ $(-\infty) + (-\infty) = -\infty,$
- ▶ $\forall n \in \mathbb{N}(-\infty + n = -\infty).$

Uwaga:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Wówczas:

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\};$

2. jeśli

$$\deg(f) \neq \deg(g),$$

to

$$\deg(f + g) = \max\{\deg(f), \deg(g)\};$$

3. $\deg(fg) \leq \deg(f) + \deg(g);$

4. jeśli

$$f \neq 0 \wedge g \neq 0 \wedge (a_n \text{ jest regularny} \vee b_m \text{ jest regularny}),$$

to

$$\deg(fg) = \deg(f) + \deg(g);$$

5. jeśli

$f \neq 0 \wedge g \neq 0 \wedge R$ jest pierścieniem całkowitym,

to

$$\deg(fg) = \deg(f) + \deg(g).$$

Dowód:

1. Niech $h = f + g = \sum_{k=0}^{\infty} c_k x^k$, przy czym $c_k = 0$ dla prawie wszystkich $k \in \mathbb{N}$.

Ustalmy $k > \max\{n, m\} = \max\{\deg(f), \deg(g)\}$.

Wówczas:

$$c_k = a_k + b_k = 0 + 0 = 0.$$

Wobec tego $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

2. Oczywiste.

3. Niech $h = f \cdot g = \sum_{k=0}^{\infty} c_k x^k$, przy czym $c_k = 0$ dla prawie wszystkich $k \in \mathbb{N}$.

Ustalmy $k > n + m = \deg(f) + \deg(g)$.

Mamy

$$c_k = \sum_{i=0}^k a_{k-i} b_i.$$

Jeżeli $i \in \{0, \dots, m\}$, to $k - i \in \{n + 1, \dots, k\}$, więc $a_{k-i} = 0$.

Podobnie, jeżeli $i \in \{m + 1, \dots, k\}$, to $b_i = 0$.

Zatem $c_k = 0$, a więc $\deg(fg) \leq \deg(f) + \deg(g)$.

4. Niech $h = f \cdot g = \sum_{k=0}^{\infty} c_k x^k$, przy czym $c_k = 0$ dla prawie wszystkich $k \in \mathbb{N}$.

Mamy

$$\begin{aligned} c_{n+m} &= \sum_{i=0}^{n+m} a_{n+m-i} b_i \\ &= \underbrace{a_{n+m}}_{=0} b_0 + \underbrace{a_{n+m-1}}_{=0} b_1 + \dots + a_n b_m + \\ &+ a_{n-1} \underbrace{b_{m+1}}_{=0} + \dots + a_0 \underbrace{b_{n+m}}_{=0} \\ &= a_n b_m. \end{aligned}$$

Ponieważ a_n lub b_m jest regularny, więc $c_{n+m} \neq 0$.

5. Wynika wprost z (4).

Wniosek:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R .

Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x].$$

Wówczas:

1. jeśli a_n jest regularny w R , to f jest regularny w $R[x]$;
2. każdy wielomian unormowany jest elementem regularnym w $R[x]$;
3. jeśli R jest całkowity, to $R[x]$ jest całkowity.

Twierdzenie o dzieleniu wielomianów z resztą:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R .

Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Wówczas istnieją liczba $l \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q, r \in R[x]$ takie, że

$$a_n^l \cdot g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Dowód:

Jeżeli $\deg(g) = m < n = \deg(f)$, to kładziemy $l = 0$, $q = 0$,
 $r = g$.

Jeżeli $\deg(g) = m = n = \deg(f)$, to $l = 1$, $q = b_m$, $r = a_n g - b_m f$.
Istotnie, zauważmy że wówczas $\deg(r) < n = \deg(f)$.

Jeżeli $\deg(g) = m > n = \deg(f)$, to dowód prowadzimy metodą indukcji względem $\deg(g) = m$.

Założmy, że dla $m_1 \in \{n+1, \dots, m-1\}$ i dla wielomianów postaci

$$g_1 = b'_0 + b'_1x + \dots + b_{m'}x^{m'} \in R[x]$$

istnieją liczba $l_1 \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q_1, r_1 \in R[x]$ takie, że

$$a_n^{l_1} \cdot g_1 = q_1 \cdot f + r_1$$

oraz $\deg(r_1) < \deg(f)$.

Położmy

$$g_1 = a_n g - b_m x^{m-n} f.$$

Wówczas

$$\deg(g_1) \in \{n+1, \dots, m-1\},$$

zatem istnieją liczba $l_1 \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q_1, r_1 \in R[x]$ takie, że

$$a_n^{l_1} \cdot g_1 = q_1 \cdot f + r_1 \text{ oraz } \deg(r_1) < \deg(f),$$

czyli

$$a_n^{l_1} \cdot (a_n g - b_m x^{m-n} f) = q_1 \cdot f + r_1 \text{ oraz } \deg(r_1) < \deg(f),$$

lub równoważnie

$$a_n^{l_1+1} g = \left(q_1 + a_n^{l_1} b_m x^{m-n} \right) \cdot f + r_1 \text{ oraz } \deg(r_1) < \deg(f).$$

Tym samym kładąc $l = l_1 + 1$, $q = q_1 + a_n^{l_1} b_m x^{m-n}$ oraz $r = r_1$ otrzymujemy tezę.

Wniosek:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R .

Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Wówczas:

1. jeśli $a_n = 1$, to istnieją wielomiany $q, r \in R[x]$ takie, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$;

2. jeśli R jest ciałem, to istnieją wielomiany $q, r \in R[x]$ takie, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Dowód:

1. Oczywiste.
2. Jeżeli R jest ciałem, to istnieje element $a_n^{-1} \in R$, a więc taki, że $a_n^{-1}a_n = 1$.

Wobec tego istnieją wielomiany $q_1, r_1 \in R[x]$ takie, że

$$g_1 = q_1 \cdot a_n^{-1}f + r_1$$

oraz $\deg(r_1) < \deg(a_n^{-1}f) = \deg(f)$.

Zatem kładąc $q = q_1 a_n^{-1}$ oraz $r = r_1$ otrzymujemy tezę.

Twierdzenie o jednoznaczności dzielenia z resztą:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R .

Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Jeśli a_n jest regularny, to istnieje co najwyżej jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Dowód:

Niech

$$g = q_1 \cdot f + r_1, \deg(r_1) < \deg f, q_1, r_1 \in R[x],$$

$$g = q_2 \cdot f + r_2, \deg(r_2) < \deg f, q_2, r_2 \in R[x].$$

Stąd

$$0 = (q_1 - q_2)f + (r_1 - r_2),$$

lub równoważnie

$$r_2 - r_1 = (q_1 - q_2)f.$$

Wobec tego:

$$\begin{aligned} \deg(f) &> \max\{\deg(r_1), \deg(r_2)\} \geq \deg(r_2 - r_1) \\ &= \deg((q_1 - q_2)f) = \deg(q_1 - q_2) + \deg(f). \end{aligned}$$

Tym samym $\deg(q_1 - q_2) = -\infty$, a więc $q_1 - q_2 = 0$, skąd też $r_2 = r_1$.

Wniosek:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

1. Jeżeli R jest całkowity, to istnieje co najwyżej jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

2. Jeżeli $a_n = 1$, to istnieje dokładnie jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

3. Jeżeli R jest ciałem, to istnieje dokładnie jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Definicja:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Jeżeli istnieje dokładnie jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$ to mówimy, że w pierścieniu $R[x]$ wykonalne jest **dzielenie z resztą** wielomianu g przez f .

Wielomian q nazywamy wówczas **niepełnym ilorazem**, a wielomian r **resztą** z dzielenia.

Uwaga i definicja:

Niech $(R, +, \cdot)$ będzie dowolnym pierścieniem.

Wielomianem zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R będziemy nazywali wyrażenie postaci

$$\sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n},$$

gdzie $m \in \mathbb{N}$, wskaźniki $i_1, \dots, i_n \in \mathbb{N}$ przebiegają wszystkie liczby nie większe niż m oraz $a_{i_1 \dots i_n} \in R$.

Dwa wielomiany uważamy za **równe**, gdy różnią się jedynie o składniki postaci $0 \cdot x_1^{i_1} \dots x_n^{i_n}$, gdzie $i_1, \dots, i_n \in \mathbb{N}$.

Będziemy mówili, że wielomian $f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ jest **stopnia** r , gdy istnieje taki różny od zera współczynnik $a_{i_1 \dots i_n}$, że $i_1 + \dots + i_n = r$ i $a_{j_1 \dots j_n} = 0$ o ile $j_1 + \dots + j_n > r$.

Umowa ta nie określa stopnia wielomianu 0, przyjmujemy więc dodatkowo, że stopniem wielomianu 0 jest $-\infty$.

Stopień wielomianu f będziemy oznaczać przez $\deg(f)$.

Wielomiany stopnia 1 będziemy nazywali **liniowymi**, a wielomiany stopnia 2 **kwadratowymi**.

Wielomian postaci $ax_1^{i_1} \dots x_n^{i_n}$, gdzie $a \in R$ oraz $i_1, \dots, i_n \in \mathbb{N}$ nazywamy **jednomianem**.

W zbiorze wszystkich wielomianów zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R definiujemy dodawanie $+$ i mnożenie $\cdot$, kładąc dla dowolnych wielomianów

$$f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \text{ oraz } g = \sum_{j_1, \dots, j_n \leq r} b_{j_1 \dots j_n} x_1^{j_1} \dots x_n^{j_n}:$$

$$f + g = \sum_{k_1, \dots, k_n \leq \max\{m, r\}} c_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n},$$

gdzie

$$c_{k_1 \dots k_n} = \begin{cases} a_{k_1 \dots k_n} + b_{k_1 \dots k_n}, & \text{gdy } k_1, \dots, k_n \leq \max\{m, r\}, \\ a_{k_1 \dots k_n}, & \text{gdy, dla pewnego wskaźnika } k_i \\ & (i \in \{1, \dots, n\}), k_i > r, \text{ ale } k_1, \dots, k_n < m, \\ b_{k_1 \dots k_n}, & \text{gdy, dla pewnego wskaźnika } k_i \\ & (i \in \{1, \dots, n\}), k_i > m, \text{ ale } k_1, \dots, k_n < r, \end{cases}$$

$$f \cdot g = \sum_{k_1, \dots, k_n \leq m+r} c_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n},$$

gdzie

$$c_{k_1 \dots k_n} = \sum_{0 \leq l_1 \leq k_1, \dots, 0 \leq l_n \leq k_n} a_{k_1 - l_1, \dots, k_n - l_n} b_{l_1, \dots, l_n}.$$

Ponadto wyróżniamy wielomian 0 jako element neutralny dodawania oraz wielomian 1 jako element neutralny mnożenia. Wówczas zbiór wszystkich wielomianów zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R z tak określonymi działaniami i wyróżnionymi elementami jest pierścieniem przemiennym z jedynek. Pierścień ten będziemy nazywali **pierścieniem wielomianów zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R** i będziemy oznaczali przez $R[x_1, \dots, x_n]$.

Konstrukcja ciał p^n -elementowych

Definicja:

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:

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 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 załóżmy, 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

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

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:

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 $g \in (h)$.

Definicja:

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:

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

$$1 + (2) = \{1, 3, 5\} = W,$$

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

$$3 + (2) = \{1, 3, 5\} = W,$$

$$4 + (2) = (2),$$

$$5 + (2) = W.$$

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

$$0 + (3) = (3),$$

$$1 + (3) = \{1, 4, 7, 10, \dots, -2, -5, -8, \dots\} = W_1,$$

$$2 + (3) = \{2, 5, 8, 11, \dots, -1, -4, -7, \dots\} = W_2,$$

$$3 + (3) = (3).$$

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:

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 notacyjna:

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