

9. WYKŁAD 9: WIELOMIANY WIELU ZMIENNYCH. WIELOMIANY SYMETRYCZNE. KONSTRUKCJA PIERŚCIEŃCIA UŁAMKÓW WZGLĘDEM ZBIORU MULTIPLIKATYWNEGO.

9.1. Wielomiany wielu zmiennych.

Definicja i Uwaga 9.1. Niech R 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 $0 \cdot x^{i_1} \dots x^{i_n}$, gdzie $i_1, \dots, i_n \in \mathbb{N}$.

Bedziemy 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 $a \cdot x_1^{i_1} \dots x_n^{i_n}$, 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 $f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ 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

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

oraz

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

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 przemienym z jedynką. Pierścień ten będziemy nazywali **pierścieniem wielomianów** zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R i będziemy oznaczali przez $R[x_1, \dots, x_n]$.

Uwaga 9.1. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Niech ponadto

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

Wówczas:

- (1) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$;
- (2) $\deg(fg) \leq \deg(f) + \deg(g)$;
- (3) jeśli

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

to

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

Wniosek 9.1. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Wówczas jeśli R jest pierścieniem całkowitym, to $R[x_1, \dots, x_n]$ też.

Definicja 9.1. Niech R i P będą dowolnymi pierścieniami, niech $R \subset P$ i niech $S \subset P$ będzie pewnym zbiorem. Zbiór S nazywamy **algebraicznie niezależnym nad R** , jeżeli zbiór

$$\{f \in R[s_1, \dots, s_n] : n \in \mathbb{N}, s_1, \dots, s_n \in S, f \text{ jest jednomianem}\}$$

jest liniowo niezależny nad pierścieniem R .

Twierdzenie 9.1 (własność uniwersalna pierścienia wielomianów wielu zmiennych). Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R .

- (1) Pierścień R ma następującą własność:

$\forall P$ – pierścień $\forall r_1, \dots, r_n \in P \forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : R[x_1, \dots, x_n] \rightarrow P$

$$[\psi(x_i) = r_i, i \in \{1, \dots, n\} \wedge \psi \upharpoonright_R = \phi].$$

- (2) Dla dowolnego rozszerzenia $R \subset S$ oraz elementów $s_1, \dots, s_n \in S \setminus R$ algebraicznie niezależnych nad R i takich, że $S = R[s_1, \dots, s_n]$, jeżeli

$\forall P$ – pierścień $\forall r_1, \dots, r_n \in P \forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : S \rightarrow P$

$$[\psi(s_i) = r_i, i \in \{1, \dots, n\} \wedge \psi \upharpoonright_R = \phi].$$

to $S \cong R[x_1, \dots, x_n]$ i izomorfizm $\alpha : R[x_1, \dots, x_n] \rightarrow S$ jest jednoznacznie wyznaczony przez warunki

$$\alpha(x_i) = s_i, i \in \{1, \dots, n\} \text{ oraz } \alpha \upharpoonright_R = \text{id}_R.$$

Definicja 9.2. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R .

- (1) Dla dowolnego pierścienia P i jego elementu $r \in P$ oraz homomorfizmu $\phi : R \rightarrow P$, jedyne przedłużenie $\psi : R[x_1, \dots, x_n] \rightarrow P$ homomorfizmu ϕ takie, że

$$[\psi(x_i) = r_i, i \in \{1, \dots, n\} \wedge \psi \upharpoonright_R = \phi]$$

nazywamy **wartością wielomianów**, a jego wartość dla wielomianu $f \in R[x_1, \dots, x_n]$, $\psi(f)$, **wartością wielomianu f w punkcie $(r_1, \dots, r_n) \in R^n$** . Jeżeli wartość wielomianu f w punkcie $(r_1, \dots, r_n) \in R^n$ jest równa 0, to punkt $(r_1, \dots, r_n) \in R^n$ nazywamy **miejszem zerowym** (lub **pierwiastkiem**) f . Najczęściej rozważamy przypadek, gdy $R = P$ oraz $\phi = \text{id}_P$. Wówczas

$$\psi(f) = \psi \left(\sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \right) = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} r_1^{i_1} \dots r_n^{i_n}.$$

(2) Dla pierścienia R^{R^n} i jego elementów $\pi_1, \dots, \pi_n \in R^{R^n}$ takich, że

$$\pi_j(a_1, a_2, \dots, a_j, \dots, a_n) = a_j, (a_1, \dots, a_n) \in R^n, j \in \{1, \dots, n\},$$

oraz homomorfizmu $\phi : R \rightarrow R^{R^n}$ danego wzorem

$$\phi(a) = \text{const.}a, \text{ dla } a \in R,$$

obraz $\psi(R[x_1, \dots, x_n])$ poprzez jedyne przedłużenie $\psi : R[x_1, \dots, x_n] \rightarrow R^{R^n}$ homomorfizmu ϕ takie, że

$$\psi(x_i) = \pi_i, i \in \{1, \dots, n\} \text{ oraz } \psi \upharpoonright_R = \phi$$

nazwamy **pierścieniem funkcji wielomianowych** o współczynnikach z R , a jego elementy **funkcjami wielomianowymi**.

Definicja i Uwaga 9.2. Niech R, P będą pierścieniami, a $\phi : P \rightarrow R$ homomorfizmem pierścieni. Wówczas istnieje dokładnie jeden homomorfizm $\psi : R[x_1, \dots, x_n] \rightarrow P[y_1, \dots, y_n]$ taki, że

$$\psi(x_i) = y_i, i \in \{1, \dots, n\} \text{ oraz } \psi \upharpoonright_R = \phi.$$

Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy, a jeśli ϕ jest surjektywny, to ψ jest surjektywny. Homomorfizm ψ nazywamy **homomorfizmem pierścieni wielomianów n zmiennych indukowanym przez homomorfizm współczynników**.

Wniosek 9.2. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Niech ponadto $0 \neq f \in R[x_1, \dots, x_n]$. Wówczas:

- (1) jeśli R jest nieskończony, to dla pewnego $(r_1, \dots, r_n) \in R^n$, $f(r_1, \dots, r_n) \neq 0$;
- (2) jeśli R jest nieskończony, to jedyny homomorfizm $\psi : R[x_1, \dots, x_n] \rightarrow R^{R^n}$ definiujący pierścień funkcji wielomianowych jest różnowartościowy.

Definicja 9.3. Niech $(I, <)$ będzie zbiorem częściowo uporządkowanym. Jeżeli

$$\forall i, j \in I \exists k \in I [i < k \wedge j < k],$$

to wówczas $(I, <)$ nazywamy **zbiorem skierowanym**.

Uwaga 9.2. Niech $(I, <)$ będzie zbiorem skierowanym, niech $\{R_i : i \in I\}$ będzie rodziną pierścieni indeksowaną elementami zbioru I taką, że

$$\forall i, j \in I [(i < j) \Rightarrow (R_i < R_j)].$$

W zbiorze $\bigcup_{i \in I} R_i$ definiujemy działania $+$ oraz $\cdot$ następująco:

- jeśli $a, b \in \bigcup_{i \in I} R_i$, to $a \in R_i$, $b \in R_j$, dla pewnych $i, j \in I$; ponieważ I jest skierowany, więc dla pewnego $k \in I$ zachodzi $i < k$ oraz $j < k$, a zatem $R_i < R_k$ oraz $R_j < R_k$, więc $a, b \in R_k$ i możemy zdefiniować

$$a + b = a +_{R_k} b \text{ oraz } a \cdot b = a \cdot_{R_k} b.$$

Wówczas $(\bigcup_{i \in I} R_i, +, \cdot)$ jest pierścieniem.

Definicja i Uwaga 9.3. Niech R będzie pierścieniem, S pewnym zbiorem, a $\{x_s : s \in S\}$ rodziną zmiennych indeksowaną elementami zbioru S . Dla dowolnego skończonego zbioru $T = \{s_1, \dots, s_n\} \subset S$ definiujemy

$$R_T = R[x_{s_1}, \dots, x_{s_n}].$$

Wówczas $(I, \subset)$, gdzie $I = \{T \subset S : \text{card} T < \infty\}$ jest zbiorem indeksowanym, zaś $\{R_T : T \in I\}$ rodziną pierścieni indeksowaną elementami zbioru I taką, że

$$\forall T_1, T_2 \in I [(T_1 \subset T_2) \Rightarrow (R_{T_1} < R_{T_2})].$$

Wobec poprzedniej uwagi $\bigcup_{T \in I} R_T$ jest pierścieniem. Nazywamy go **pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z R** i oznaczamy $R[\{x_s : s \in S\}]$.

Uwaga 9.3. Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R . Niech ponadto

$$f \in R[\{x_s : s \in S\}] \text{ oraz } g \in R[\{x_s : s \in S\}].$$

Wówczas:

- (1) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$;
- (2) $\deg(fg) \leq \deg(f) + \deg(g)$;
- (3) jeśli

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

to

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

Wniosek 9.3. Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R . Wówczas jeśli R jest pierścieniem całkowitym, to $R[\{x_s : s \in S\}]$ też.

Twierdzenie 9.2 (własność uniwersalna pierścienia wielomianów nieskończonej liczby zmiennych). Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R .

- (1) Pierścień R ma następującą własność:

$\forall P$ – pierścień $\forall \lambda : \{x_s : s \in S\} \rightarrow P$ – odwzorowanie $\forall \phi : R \rightarrow P$ – homomorfizm $\exists ! \psi : R[\{x_s : s \in S\}] \rightarrow P$

$$[\psi \upharpoonright_{\{x_s : s \in S\}} = \lambda \wedge \psi \upharpoonright_R = \phi].$$

- (2) Dla dowolnego rozszerzenia $R \subset R'$ i zbioru $T \subset R'$ algebraicznie niezależnego nad R i takiego, że $R' = R[\{x_t : t \in T\}]$, jeżeli

$\forall P$ – pierścień $\forall \lambda : \{x_t : t \in T\} \rightarrow P$ – odwzorowanie $\forall \phi : R \rightarrow P$ – homomorfizm $\exists ! \psi : R' \rightarrow P$

$$[\psi \upharpoonright_{\{x_t : t \in T\}} = \lambda \wedge \psi \upharpoonright_R = \phi].$$

to $R' \cong R[\{x_t : t \in T\}]$ i izomorfizm $\alpha : R[\{x_t : t \in T\}] \rightarrow R'$ jest jednoznacznie wyznaczony przez warunki

$$\alpha(x_t) = t, t \in T \text{ oraz } \alpha \upharpoonright_R = id_R.$$

Definicja 9.4. Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R . Dla dowolnego pierścienia P i odwzorowania $\lambda : \{x_s : s \in S\} \rightarrow P$ oraz homomorfizmu $\phi : R \rightarrow P$, jedyne przedłużenie $\psi : R[\{x_s : s \in S\}] \rightarrow P$ homomorfizmu ϕ takie, że

$$[\psi \upharpoonright_{\{x_s : s \in S\}} = \lambda \wedge \psi \upharpoonright_R = \phi]$$

nazwamy **wartością wielomianów**, a jego wartość dla wielomianu $f \in R[\{x_s : s \in S\}]$, $\psi(f)$, **wartością wielomianu f na zbiorze $\lambda(\{x_s : s \in S\}) \subset P$** . Jeżeli wartość wielomianu f na zbiorze $\lambda(\{x_s : s \in S\}) \subset P$ jest równa 0, to zbiór $\lambda(\{x_s : s \in S\}) \subset P$ nazywamy **miejszem zerowym** (lub **pierwiastkiem**) f . Najczęściej rozważamy przypadek, gdy $R = P$ oraz $\phi = id_P$.

Definicja i Uwaga 9.4. Niech R, P będą pierścieniami, S pewnym zbiorem, a $\phi : P \rightarrow R$ homomorfizmem pierścieni. Wówczas istnieje dokładnie jeden homomorfizm $\psi : R[\{x_s : s \in S\}] \rightarrow P[\{y_s : s \in S\}]$ taki, że

$$\psi(x_s) = y_s, s \in S \text{ oraz } \psi \upharpoonright_R = \phi.$$

Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy, a jeśli ϕ jest surjektywny, to ψ jest surjektywny. Homomorfizm ψ nazywamy **homomorfizmem pierścieni wielomianów n zmiennych indukowanym przez homomorfizm współczynników**.

Definicja 9.5. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Wielomian

$$0 \neq f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in R[x_1, \dots, x_n]$$

nazywamy **wielomianem jednorodnym stopnia d (lub formą stopnia d)** jeżeli

$$\forall i_1, \dots, i_n \leq m [\deg(a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}) = d].$$

Formy stopnia 1 nazywamy **formami liniowymi**, formy stopnia 2 **formami kwadratowymi**, formy stopnia 3 **formami kubicznymi** itd.

Uwaga 9.4. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Wielomian

$$0 \neq f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in R[x_1, \dots, x_n]$$

jest wielomianem jednorodnym stopnia d wtedy i tylko wtedy, gdy dla każdego pierścienia P , $R < P$ i dla każdego zbioru $n+1$ algebraicznie niezależnych nad R elementów $a, b_1, \dots, b_n \in P$ zachodzi równość

$$f(ab_1, \dots, ab_n) = a^d f(b_1, \dots, b_n).$$

9.2. Wielomiany symetryczne.

Definicja 9.6. Niech $n \in \mathbb{N}$, niech R będzie pierścieniem.

(1) Wielomian $f \in R[x_1, \dots, x_n]$ nazywamy **wielomianem półsymetrycznym**, jeżeli

$$\forall \sigma \in A(n) [f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})].$$

(2) Wielomian $f \in R[x_1, \dots, x_n]$ nazywamy **wielomianem symetrycznym**, jeżeli

$$\forall \sigma \in S(n) [f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})].$$

Zbiór wszystkich wielomianów symetrycznych oznaczamy $R_{\text{sym}}[x_1, \dots, x_n]$.

Przykłady:

- (1) Rozważmy $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x + 3^2$. Jest to wielomian symetryczny.
- (2) Rozważmy $f(x_1, x_2, x_3) = x_1 x_2 x_3$. Jest to wielomian symetryczny.
- (3) Rozważmy $V(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$. Jest to wielomian półsymetryczny, nazywamy go **wielomianem Vandermonde'a**.
- (4) Rozważmy $V^2(x_1, \dots, x_n)$. Jest to wielomian symetryczny.

Uwaga 9.5. Niech $n \in \mathbb{N}$, niech R będzie pierścieniem. Wówczas $R_{\text{sym}}[x_1, \dots, x_n]$ jest pierścieniem.

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja 9.7. Niech $n \in \mathbb{N}$, niech R będzie pierścieniem. Wielomiany:

$$\begin{aligned} S_1(x_1, \dots, x_n) &= x_1 + \dots + x_n \\ S_2(x_1, \dots, x_n) &= x_1x_2 + \dots + x_1x_n + x_2x_3 + \dots + x_2x_n + \dots + x_{n-1}x_n \\ &\vdots \\ S_k(x_1, \dots, x_n) &= \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1}x_{i_2} \dots x_{i_k} \\ &\vdots \\ S_n(x_1, \dots, x_n) &= x_1 \dots x_n. \end{aligned}$$

nazywamy wielomianami symetrycznymi podstawowymi zmiennych $x_1, \dots, x_n$.

Twierdzenie 9.3. Niech $n \in \mathbb{N}$, niech F będzie ciałem. Wówczas wielomiany symetryczne podstawowe $S_1, \dots, S_n \in F_{\text{sym}}[x_1, \dots, x_n]$ są algebraicznie niezależne nad F .

Dowód. Dowód prowadzimy przez indukcję względem n . Dla $n = 1$ teza jest oczywista, założmy więc, że $n > 1$ i że wielomiany symetryczne podstawowe $n - 1$ zmiennych $S'_1, \dots, S'_{n-1} \in F_{\text{sym}}[x_1, \dots, x'_{n-1}]$ są algebraicznie niezależne. Przypuśćmy nie wprost, że istnieje wielomian $\lambda \in F[y_1, \dots, y_n]$ taki, że

$$\lambda(S_1, \dots, S_n) = 0.$$

Niech ponadto λ będzie wielomianem możliwie najniższego stopnia. Oczywiście $S_j(x_1, \dots, x_{n-1}, 0) = S'_j(x_1, \dots, x_{n-1})$, dla $j \in \{1, \dots, n-1\}$. Ponadto $S_n(x_1, \dots, x_{n-1}, 0) = 0$. Niech

$$\lambda(y_1, \dots, y_n) = \psi_0(y_1, \dots, y_{n-1})y_n^n + \psi_1(y_1, \dots, y_{n-1})y_n^{n-1} + \dots + \psi_n(y_1, \dots, y_{n-1}).$$

Wobec tego:

$$\begin{aligned} 0 &= \lambda(S_1(x_1, \dots, x_{n-1}, 0), \dots, S_n(x_1, \dots, x_{n-1}, 0)) \\ &= \lambda(S'_1(x_1, \dots, x_{n-1}), \dots, S'_{n-1}(x_1, \dots, x_{n-1}), S_n(x_1, \dots, x_{n-1}, 0)) \\ &= \psi_0(S'_1(x_1, \dots, x_{n-1}), \dots, S'_{n-1}(x_1, \dots, x_{n-1}))0^n + \\ &\quad + \psi_n(S'_1(x_1, \dots, x_{n-1}), \dots, S'_{n-1}(x_1, \dots, x_{n-1})) \\ &= \psi_n(S'_1(x_1, \dots, x_{n-1}), \dots, S'_{n-1}(x_1, \dots, x_{n-1})). \end{aligned}$$

Ponieważ $S'_1, \dots, S'_{n-1}$ są algebraicznie niezależne, więc $\psi_n = 0$. Wobec tego:

$$\lambda(y_1, \dots, y_n) = y_n(\psi_0(y_1, \dots, y_{n-1})y_n^{n-1} + \psi_1(y_1, \dots, y_{n-1})y_n^{n-2} + \dots + \psi_{n-1}(y_1, \dots, y_{n-1})),$$

a zatem

$$\psi_0(S_1, \dots, S_{n-1})S_n^{n-1} + \psi_1(S_1, \dots, S_{n-1})S_n^{n-2} + \dots + \psi_{n-1}(S_1, \dots, S_{n-1}) = 0$$

i stopień wielomianu $\psi_0(y_1, \dots, y_{n-1})y_n^{n-1} + \psi_1(y_1, \dots, y_{n-1})y_n^{n-2} + \dots + \psi_{n-1}(y_1, \dots, y_{n-1})$ jest mniejszy od stopnia wielomianu λ , zatem $\psi_0 = 0, \dots, \psi_{n-1} = 0$ i tym samym λ jest wielomianem zerowym, co daje sprzeczność. $\square$

Twierdzenie 9.4 (zasadnicze twierdzenie teorii wielomianów symetrycznych). Niech $n \in \mathbb{N}$, niech F będzie ciałem. Wówczas wielomiany symetryczne podstawowe $S_1, \dots, S_n \in F_{\text{sym}}[x_1, \dots, x_n]$ generują pierścień $F_{\text{sym}}[x_1, \dots, x_n]$.

Dowód. Wystarczy pokazać, że dla ustalonego wielomianu symetrycznego $f \in F_{\text{sym}}[x_1, \dots, x_n]$ istnieje wielomian $G \in F[y_1, \dots, y_n]$ taki, że:

$$f = G(S_1, \dots, S_n).$$

Dowód prowadzimy przez indukcję względem n . Dla $n = 1$ teza jest oczywista, ustalmy więc $n > 1$ i założmy, że twierdzenie jest prawdziwe dla wszelkich $k < n$. Niech $m = \deg f$. Konstrukcję wielomianu G prowadzimy indukcyjnie względem m . Znowu, dla $m = 1$ nie ma co robić, założmy więc, że $m > 1$ i że stosowne wielomiany G zostały już skonstruowane dla f o stopniu $l < m$.

Wielomian $f(x_1, \dots, x_{n-1}, 0) \in F[x_1, \dots, x_n]$ jest wielomianem symetrycznym $n-1$ zmiennych. Wobec założenia indukcyjnego istnieje wielomian $G_1 \in F[y_1, \dots, y_{n-1}]$ taki, że

$$f(x_1, \dots, x_{n-1}, 0) = G_1(S'_1(x_1, \dots, x_{n-1}), \dots, S_{n-1}'(x_1, \dots, x_{n-1})),$$

gdzie $S'_1(x_1, \dots, x_{n-1}), \dots, S'_{n-1}(x_1, \dots, x_{n-1}) \in F[x_1, \dots, x_{n-1}]$ są wielomianami symetrycznymi podstawowymi $n-1$ zmiennych. Niech

$$f_1(x_1, \dots, x_n) = f(x_1, \dots, x_n) - G_1(S_1(x_1, \dots, x_n), \dots, S_n(x_1, \dots, x_n)).$$

Wówczas f_1 jest wielomianem symetrycznym. Ponadto $f_1(x_1, \dots, x_{n-1}, 0) = 0$, więc $x_n | f_1$. Istnieje zatem $h \in F[x_1, \dots, x_n]$ taki, że

$$f_1(x_1, \dots, x_n) = x_n h(x_1, \dots, x_n).$$

Ustalmy $k \in \{1, \dots, n\}$ i niech $\sigma = (k, n) \in S(n)$. Wówczas:

$$f_1(x_1, \dots, x_n) = f_1(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = x_k h(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Wobec tego $x_k | f_1(x_1, \dots, x_n)$, dla $k \in \{1, \dots, n\}$. Ponieważ wielomiany $x_1, \dots, x_n$ są parami względnie pierwsze, więc w rezultacie $x_1 \dots x_n | f_1(x_1, \dots, x_n)$, czyli $S_n(x_1, \dots, x_n) | f_1(x_1, \dots, x_n)$. Istnieje zatem $g \in F[x_1, \dots, x_n]$ taki, że

$$f_1(x_1, \dots, x_n) = S_n(x_1, \dots, x_n) g(x_1, \dots, x_n).$$

Oczywiście $g(x_1, \dots, x_n)$ jest wielomianem symetrycznym. Ponadto $\deg g = \deg f_1 - \deg S_n = \deg f_1 - n < m$. Wobec założenia indukcyjnego istnieje wielomian $G_2 \in F[y_1, \dots, y_n]$ taki, że

$$g(x_1, \dots, x_n) = G_2(S_1(x_1, \dots, x_n), \dots, S_n(x_1, \dots, x_n)).$$

Zatem $f_1(x_1, \dots, x_n) = S_n(x_1, \dots, x_n) G_2(S_1(x_1, \dots, x_n), \dots, S_n(x_1, \dots, x_n))$, skąd

$$f(x_1, \dots, x_n) = G_1(S_1(x_1, \dots, x_n), \dots, S_{n-1}(x_1, \dots, x_n)) + S_n(x_1, \dots, x_n) G_2(S_1(x_1, \dots, x_n), \dots, S_n(x_1, \dots, x_n)),$$

czyli $G = G_1 + y_n G_2$. □

Zauważmy przy okazji, że wielomian G jest wyznaczony w powyższym dowodzie jednoznacznie: gdyby bowiem istniały dwa wielomiany $G, G' \in F[y_1, \dots, y_n]$ takie, że:

$$G(S_1, \dots, S_n) = G'(S_1, \dots, S_n),$$

to wówczas $(G - G')(S_1, \dots, S_n) = 0$, co, wobec algebraicznej niezależności $S_1, \dots, S_n$, daje $G - G' = 0$, czyli $G = G'$.

Przykład:

- (5) Rozważmy $f(x_1, x_2, x_3) = (x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$. Odwołując się do notacji z dowodu zasadniczego twierdzenia teorii wielomianów symetrycznych, mamy:

$$f(x_1, x_2, 0) = (x_1 + x_2)x_1x_2 = S'_1(x_1, x_2)S'_2(x_1, x_2) = G_1(S'_1, S'_2),$$

gdzie $G_1(y_1, y_2) = y_1y_2$. Wówczas

$$f_1(x_1, x_2, x_3) = f(x_1, x_2, x_3) - S_1S_2 = -x_1x_2x_3,$$

czyli $f_1(x_1, x_2, x_3) = S_3(x_1, x_2, x_3)$, $g(x_1, x_2, x_3) = 1$ oraz $G_2(y_1, y_2, y_3) = 1$. Reasumując:

$$f = S_1 S_2 - S_3.$$

9.3. Konstrukcja pierścienia ułamków względem zbioru mnożliwego.

Definicja 9.8. Niech R będzie pierścieniem. Podzbiór $S \subset R$ nazywamy **podzbiorem mnożliwym**, jeżeli

- (1) $1 \in S$, $0 \notin S$,
- (2) $\forall a, b \in S (ab \in S)$.

Przykłady:

- (1) Niech R będzie pierścieniem. Wówczas $S = U(R)$ jest podzbiorem mnożliwym.
- (2) Niech R będzie pierścieniem całkowitym. Wówczas $S = R \setminus \{0\}$ jest podzbiorem mnożliwym.
- (3) Niech R będzie pierścieniem, $I \triangleleft R$ ideałem pierwszym. Wówczas $S = R \setminus I$ jest podzbiorem mnożliwym.
- (4) Niech $R = \mathbb{Z}$. Wówczas $S = \{2^k : k \in \mathbb{N} \cup \{0\}\}$ jest podzbiorem mnożliwym.

Twierdzenie 9.5. Niech $\mathcal{R} = \{S_i : i \in I\}$ będzie rodziną podzbiorów mnożliwych pierścienia R ;

- (1) $\bigcap_{i \in I} S_i$ jest podzbiorem mnożliwym pierścienia R ,
- (2) $\bigcup_{i \in I} S_i$ jest podzbiorem mnożliwym pierścienia R , o ile $\mathcal{R}$ jest łańcuchem.

Definicja 9.9. Niech R będzie pierścieniem oraz $A \subset U(R)$ pewnym zbiorem. Najmniejszy w sensie inkluzji podzbiór mnożliwy pierścienia R zawierający zbiór A (tj. przekrój wszystkich podzbiorów mnożliwych pierścienia R zawierających A) nazywamy **podzbiorem mnożliwym generowanym przez A** .

Definicja i Uwaga 9.5. Niech R będzie pierścieniem oraz $S \subset R$ podzbiorem mnożliwym. W zbiorze $R \times S$ definiujemy relację $\sim$ warunkiem

$$(a_1, s_1) \sim (a_2, s_2) \text{ wtw. } \exists s_0 \in S [s_0(a_1 s_2 - a_2 s_1) = 0].$$

Wówczas relacja $\sim$ jest relacją równoważnościową. Klasę abstrakcji $[(a, s)]_\sim$ nazywamy **ułamkiem o liczniku a i mianowniku s** i oznaczamy $\frac{a}{s}$. Zbiór klas abstrakcji relacji $\sim$ oznaczamy przez $S^{-1}R$. W zbiorze $S^{-1}R$ definiujemy

- element zerowy

$$\frac{0}{1},$$

- jedynkę

$$\frac{1}{1},$$

- dodawanie

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2},$$

- mnożenie

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

Wówczas $(S^{-1}R)$ jest pierścieniem. Nazywamy go **pierścieniem ułamków (lokalizacją) pierścienia R względem zbioru mnożliwego S** .

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja i Uwaga 9.6. Niech R będzie pierścieniem oraz $S \subset R$ podzbiorem mnożliwym. Odwzorowanie $\lambda : R \rightarrow S^{-1}R$ dane wzorem

$$\lambda(a) = \frac{a}{1}$$

jest homomorfizmem. Nazywamy go **homomorfizmem kanonicznym**. Ponadto

$$\lambda(S) \subset U(S^{-1}R).$$

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Twierdzenie 9.6. Niech R będzie pierścieniem oraz $S \subset R$ podzbiorem mnożliwym. Homomorfizm kanoniczny $\lambda : R \rightarrow S^{-1}R$ jest różnowartościowy wtedy i tylko wtedy, gdy

$$S \subset R \setminus \mathcal{D}(R).$$

Dowód. $(\Leftarrow)$: Ustalmy $a, b \in R$ i założmy, że

$$\lambda(a) = \lambda(b).$$

Wówczas $\frac{a}{1} = \frac{b}{1}$, a zatem dla pewnego $s_0 \in S$:

$$s_0(a - b) = 0.$$

Ponieważ s_0 nie jest dzielnikiem zera, więc $a - b = 0$, czyli $a = b$.

$(\Rightarrow)$: Załóżmy, że $s_0 \in S$ jest dzielnikiem zera, czyli $s_0 a = 0$ dla pewnego $a \in R \setminus \{0\}$. Wówczas $s_0(a - 0) = 0$, czyli $\frac{a}{1} = \frac{0}{1}$, a zatem

$$\lambda(a) = \lambda(0)$$

więc λ nie jest różnowartościowy. □

Wniosek 9.4. Niech R będzie pierścieniem całkowitym oraz $S \subset R$ podzbiorem mnożliwym. Wówczas homomorfizm kanoniczny $\lambda : R \rightarrow S^{-1}R$ jest różnowartościowy.

Definicja i Uwaga 9.7. Niech R będzie pierścieniem całkowitym oraz $S = R \setminus \{0\}$. Wówczas homomorfizm kanoniczny $\lambda : R \rightarrow S^{-1}R$ jest różnowartościowy, a pierścień $S^{-1}R$ jest ciałem (to znaczy każdy pierścień całkowity można zanurzyć w ciało). Ciało $S^{-1}R$ nazywamy **ciałem ułamków** pierścienia całkowitego R i oznaczamy (R) .

Dowód. Wystarczy pokazać, że $S^{-1}R$ jest ciałem. Ustalmy $\frac{a}{s} \in S^{-1}R \setminus \{\frac{0}{1}\}$. Pokażemy, że $\frac{a}{s} \in U(S^{-1}R)$. Zauważmy, że $a \neq 0$: istotnie, przypuśćmy, że $a = 0$. Wówczas $\frac{a}{s} = \frac{0}{s} = \frac{0}{1}$, co daje sprzeczność. Wobec tego $\frac{s}{a} \in S^{-1}R$. Ponadto $\frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}$. □

Przykłady:

- (5) Niech $R = \mathbb{Z}$. Wówczas $\mathbb{Q} \cong (\mathbb{Z})$ jest ciałem ułamków $\mathbb{Z}$.
- (6) Niech $R = F[x_1, \dots, x_n]$ będzie pierścieniem wielomianów n zmiennych nad ciałem F . Wówczas ciało ułamków pierścienia R oznaczamy $F(x_1, \dots, x_n)$ i nazywamy **ciałem funkcji wymiernych** a jego elementy **funkcjami wymiernymi n zmiennych**.

Twierdzenie 9.7 (własność uniwersalna pierścienia ułamków). Niech P, R będą pierścieniami, $S \subset P$ zbiorem mnożliwym, niech $\phi : P \rightarrow R$ będzie homomorfizmem takim, że

$$\phi(S) \subset U(R).$$

Wówczas istnieje dokładnie jeden homomorfizm $\psi : S^{-1}P \rightarrow S^{-1}R$ taki, że

$$\psi \circ \lambda = \phi,$$

gdzie $\lambda : P \rightarrow S^{-1}P$ jest homomorfizmem kanonicznym. Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy. Inaczej: diagram

$$\begin{array}{ccc} P & \xrightarrow{\phi} & R \\ \lambda \downarrow & \nearrow \psi & \\ S^{-1}P & & \end{array}$$

jest przemienny.

Dowód. Zdefiniujmy odwzorowanie $\psi : S^{-1}P \rightarrow R$ wzorem

$$\psi\left(\frac{a}{s}\right) = \phi(a)(\phi(s))^{-1} \text{ dla } \frac{a}{s} \in S^{-1}P.$$

Pokażemy, że ψ jest dobrze określone. Istotnie, ustalmy $\frac{a}{s} \in S^{-1}P$ i niech $\frac{a}{s} = \frac{a'}{s'}$. Wobec tego istnieje element $s_0 \in S$ taki, że

$$s_0(as' - a's) = 0.$$

Zatem

$$\phi(s_0(as' - a's)) = \phi(s_0)(\phi(a)\phi(s') - \phi(a')\phi(s)) = 0.$$

Ponieważ $\phi(s_0) \in U(R)$, więc $\phi(a)\phi(s') - \phi(a')\phi(s) = 0$, a stąd

$$\psi\left(\frac{a}{s}\right) = \phi(a)(\phi(s))^{-1} = \phi(a')(\phi(s'))^{-1} = \psi\left(\frac{a'}{s'}\right).$$

Bez trudu sprawdzamy, że ψ jest homomorfizmem oraz że jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy. Pokażemy, że $\psi \circ \lambda = \phi$. Ustalmy w tym celu $a \in P$. Mamy:

$$\psi \circ \lambda(a) = \psi(\lambda(a)) = \psi\left(\frac{a}{1}\right) = \phi(a)(\psi(1))^{-1} = \phi(a).$$

Pozostaje wykazać, że ψ jest wyznaczone jednoznacznie. Niech bowiem $\psi_1, \psi_2 : S^{-1}P \rightarrow S^{-1}R$ będą takimi homomorfizmami, że

$$\psi_1 \circ \lambda = \phi \text{ oraz } \psi_2 \circ \lambda = \phi.$$

Ustalmy $\frac{a}{s} \in S^{-1}P$. Mamy:

$$\begin{aligned} \psi_1\left(\frac{a}{s}\right) &= \psi_1\left(\frac{a}{1} \cdot \frac{1}{s}\right) = \psi_1\left(\frac{a}{1}\right) \cdot \psi_1\left(\frac{1}{s}\right) = \psi_1\left(\frac{a}{1}\right) \cdot (\psi_1\left(\frac{s}{1}\right))^{-1} \\ &= \psi_1(\lambda(a))(\psi_1(\lambda(s)))^{-1} = \psi_1 \circ \lambda(a) \cdot (\psi_2 \circ \lambda(a))^{-1} \\ &= \phi(a)(\psi(s))^{-1} = \psi_2\left(\frac{a}{s}\right). \end{aligned}$$

□

Wniosek 9.5. Niech P będzie pierścieniem całkowitym, niech R będzie dowolnym pierścieniem, $S \subset P$ zbiorem mnożliwym, niech $\phi : P \rightarrow R$ będzie homomorfizmem takim, że

$$\phi(S) \subset U(R).$$

Wówczas istnieje dokładnie jeden homomorfizm $\psi : S^{-1}P \rightarrow S^{-1}R$ taki, że

$$\psi \circ \lambda = \phi,$$

gdzie $\lambda : P \rightarrow S^{-1}P$ jest homomorfizmem kanonicznym. Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy. Inaczej: diagram

$$\begin{array}{ccc} P & \xrightarrow{\phi} & R \\ \lambda \downarrow & \nearrow \psi & \\ S^{-1}P & & \end{array}$$

jest przemienny.

Wniosek 9.6. Niech P będzie pierścieniem całkowitym, niech F będzie dowolnym ciałem, niech $\phi : P \rightarrow F$ będzie homomorfizmem różnowartościowym. Wówczas istnieje dokładnie jeden homomorfizm różnowartościowy $\psi : (P) \rightarrow F$ taki, że

$$\psi \circ \lambda = \phi,$$

gdzie $\lambda : P \rightarrow (P)$ jest homomorfizmem kanonicznym. Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy. Inaczej: diagram

$$\begin{array}{ccc} P & \xrightarrow{\phi} & F \\ \lambda \downarrow & \nearrow \psi & \\ (P) & & \end{array}$$

jest przemienny (to znaczy dla każdego pierścienia całkowitego jego ciało ułamków jest najmniejszym ciałem, w jaki pierścień ten można zanurzyć).