PIERŚCIENIE I CIAŁA
Wykład 8

Charakterystyka pierścienia

Niech P będzie pierścieniem przemiennym z $1 \neq 0$. Dla $a \in P$ oznaczamy $0 \cdot a = 0$,

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ składników}}$$

dla $n \in \mathbb{N}$ oraz

$$n \cdot a = -((-n) \cdot a) = \underbrace{-a - a - \cdots - a}_{-n \text{ składników}}$$

dla $n \in \mathbb{Z}$, $n < 0$. Należy zwrócić uwagę, że we wzorach tych a jest elementem pierścienia P, zaś n jest liczbą całkowitą, więc $\cdot$ nie oznacza mnożenia w pierścieniu. Zauważmy, że

$$(n+m) \cdot a = n \cdot a + m \cdot a, \quad nm \cdot a = (n \cdot a)(m \cdot 1) \tag{1}$$

dla dowolnych $n, m \in \mathbb{Z}$. Ponadto

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ składników}} = a(\underbrace{1 + 1 + \cdots + 1}_{n \text{ składników}}) = a(n \cdot 1). \tag{2}$$

Zbiór $G = \{n \cdot 1 : n \in \mathbb{Z}\}$ jest podgrupą cykliczną grupy $(P, +)$ generowaną przez 1. Jeśli rząd tej podgrupy jest liczbą skończoną n, to nazywamy ją ***charakterystyką pierścienia*** P i piszemy $\operatorname{char}(P) = n$. Wtedy n jest najmniejszą liczbą naturalną taką, że

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ składników}} = 0.$$

Jeżeli k jest wielokrotnością n, czyli $k = mn$ dla pewnego $m \in \mathbb{Z}$, to z drugiego wzoru w (1) wynika, że $k \cdot 1 = mn \cdot 1 = 0$. Ze wzoru (2) wynika, że wtedy także $k \cdot a = 0$ dla każdego $a \in P$.

Jeśli podgrupa G jest nieskończona, to mówimy, że P ma charakterystykę 0 i piszemy $\operatorname{char}(P) = 0$. Oznacza to, że

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ składników}} \neq 0$$

dla każdego $n \in \mathbb{N}$.

Dla $n \in \mathbb{Z}$ przyjmujemy $f(n) = n \cdot 1$. Wzory (1) pokazują, że funkcja $f : \mathbb{Z} \to P$ jest homomorfizmem. Mamy dwa przypadki:

- $\operatorname{char}(P) = 0$. Wtedy homomorfizm f jest różnowartościowy, a więc P zawiera podpierścień $f(\mathbb{Z}) = \{n \cdot 1 : n \in \mathbb{Z}\}$ izomorficzny z $\mathbb{Z}$.
- $\operatorname{char}(P) = n > 0$. Wtedy

  $$\operatorname{Ker} f = \{m \in \mathbb{Z} : m \cdot 1 = 0\} = \{kn : k \in \mathbb{Z}\} = (n)$$

  jest ideałem w $\mathbb{Z}$ generowanym przez n. Zatem P zawiera podpierścień $f(\mathbb{Z})$ izomorficzny z $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Przykład 1. Oczywiście $\operatorname{char}(\mathbb{Z}) = 0$ i $\operatorname{char}(\mathbb{Z}_n) = n$ dla $n \in \mathbb{N}$, $n > 1$.

Twierdzenie 1. *Jeżeli P jest pierścieniem całkowitym i* $\mathrm{char}(P) = p > 0$*, to p jest liczbą pierwszą.*

Dowód. Gdyby p nie było liczbą pierwszą, to $p = kl$, gdzie $1 < k, l < p$. Mamy

$$0 = p \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1),$$

a ponieważ P jest pierścieniem całkowitym, więc $k \cdot 1 = 0$ lub $l \cdot 1 = 0$. Jest to sprzeczne z założeniem, że p jest najmniejszą liczbą naturalną, dla której $p \cdot 1 = 0$. □

W dowolnym pierścieniu przemiennym P mamy wzór dwumianowy:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k b^{n-k}, \tag{3}$$

gdzie $a, b \in P$, $n \in \mathbb{N}$. Np.

$$(a+b)^2 = a^2 + 2 \cdot ab + b^2, \quad (a+b)^3 = a^3 + 3 \cdot ab^2 + 3 \cdot a^2 b + b^3.$$

Uwaga 1. Jeżeli $p > 1$ jest liczbą pierwszą, to dla $k = 1, ..., p-1$ współczynnik $\binom{p}{k}$ dzieli się przez p.

Jeżeli więc $\mathrm{char}(P) = p$, to p jest liczbą pierwszą i powyższa uwaga oznacza, że $\binom{p}{k} \cdot 1 = 0$ dla $k = 1, ..., p-1$, co daje następującą uproszczoną wersję wzoru dwumianowego:

$$(a+b)^p = a^p + b^p. \tag{4}$$

Z twierdzenia 1 wynika, że wzór ten zachodzi w dowolnym pierścieniu całkowitym P takim, że $\mathrm{char}(P) = p$.

Ciało ułamków

Niech P będzie pierścieniem całkowitym i $P^* = P \setminus \{0\}$. W zbiorze $P \times P^*$ definiujemy relację

$$(a, u) \sim (b, w) \Leftrightarrow aw = bu,$$

gdzie $a, b \in P$, $u, w \in P^*$. Jest to relacja równoważności. Klasę abstrakcji pary $(a, u) \in P \times P^*$ względem tej relacji nazywamy ułamkiem o liczniku a i mianowniku u. Oznaczamy go przez $\frac{a}{u}$. W zbiorze $U(P)$ wszystkich takich ułamków definiujemy działania:

$$\frac{a}{u} + \frac{b}{w} = \frac{aw + bu}{uw}, \quad \frac{a}{u} \cdot \frac{b}{w} = \frac{ab}{uw}.$$

Działania te są dobrze określone, gdyż jeżeli $(a, u) \sim (a_1, u_1)$ i $(b, w) \sim (b_1, w_1)$, to

$$(aw + bu)u_1 w_1 = au_1 ww_1 + bw_1 uu_1 = a_1 uww_1 + b_1 wuu_1 = (a_1 w_1 + b_1 u_1)uw,$$

więc

$$\frac{a}{u} + \frac{b}{w} = \frac{aw + bu}{uw} = \frac{a_1 w_1 + b_1 u_1}{u_1 w_1} = \frac{a_1}{u_1} + \frac{b_1}{w_1} \tag{5}$$

oraz $abu_1 w_1 = a_1 b_1 uw$, więc

$$\frac{a}{u} \cdot \frac{b}{w} = \frac{ab}{uw} = \frac{a_1 b_1}{u_1 w_1} = \frac{a_1}{u_1} \cdot \frac{b_1}{w_1}. \tag{6}$$

Zbiór ułamków $U(P)$ z tymi działaniami jest ciałem. Nazywamy go ***ciałem ułamków*** pierścienia całkowitego P. Jego zerem jest $\frac{0}{1}$, a jedynką jest $\frac{1}{1}$. Funkcja $f : P \to U(P)$

określona wzorem $f(x) = \frac{x}{1}$ jest różnowartościowym homomorfizmem. Utożsamiając x z $f(x) = \frac{x}{1}$ możemy uważać P za podpierścień ciała $U(P)$.

Przykład 2. Powyższa konstrukcja ciała ułamków jest uogólnieniem konstrukcji ciała liczb wymiernych $\mathbb{Q}$. Jest to ciało ułamków pierścienia $\mathbb{Z}$.

Dla dowolnego $d \in \mathbb{C}$ ciało $\mathbb{Q}[\sqrt{d}]$ jest ciałem ułamków pierścienia $\mathbb{Z}[\sqrt{d}]$.

Dla dowolnego pierścienia całkowitego P ciało ułamków pierścienia wielomianów $P[x]$ nazywamy ***ciałem funkcji wymiernych***.

Pierwiastki wielomianu

Niech P będzie pierścieniem przemiennym z $1 \neq 0$ i $f \in P[x]$. Element $a \in P$ jest pierwiastkiem wielomianu f, jeśli $f(a) = 0$.

Twierdzenie 2 (twierdzenie Bézouta)**.** *Element $a \in P$ jest pierwiastkiem wielomianu $f \in P[x]$ wtedy i tyko wtedy, gdy f dzieli się przez $x - a$.*

Dowód. Załóżmy, że a jest pierwiastkiem wielomianu f. Dzieląc f z resztą przez $x - a$ otrzymujemy resztę $r = f(a) = 0$, czyli f dzieli się przez $x - a$.

Załóżmy teraz, że f dzieli się przez $x - a$. Wtedy $f = (x - a)q$ dla pewnego $q \in P[x]$ i wstawiając a w miejsce x otrzymujemy $f(a) = (a - a)q(a) = 0$. □

Liczbę k nazywamy ***krotnością pierwiastka*** a wielomianu f jeśli f dzieli się przez $(x-a)^k$ i f nie dzieli się przez $(x-a)^{k+1}$. Jeśli krotność pierwiastka a jest większa niż 1, to mówimy, że a jest ***pierwiastkiem wielokrotnym***. Pierwiastek o krotności 1 nazywamy ***pierwiastkiem pojedynczym***.

Twierdzenie 3. *Niech $a \in P$ będzie pierwiastkiem wielomianu $f \in P[x]$. Pierwiastek a ma krotność k wtedy i tyko wtedy, gdy $f = (x - a)^k g$ dla pewnego $g \in P[x]$ takiego, że $g(a) \neq 0$.*

Dowód. Załóżmy, że pierwiastek a ma krotność k i $f = (x - a)^k g$ przy czym $g(a) = 0$. Wtedy g dzieli się przez $x - a$, a więc $g = (x - a)h$ dla pewnego $h \in P[x]$. Stąd $f = (x - a)^{k+1}h$, zatem krotność a jest większa niż k, co jest sprzeczne z założeniem. Stąd $g(a) \neq 0$.

Na odwrót, załóżmy, że $f = (x - a)^k g$ i $g(a) \neq 0$. Gdyby pierwiastek a miał krotność większą niż k, to mielibyśmy $f = (x - a)^{k+1}h$ dla pewnego $h \in P[x]$. Wtedy

$$(x - a)^k g = (x - a)^{k+1}h,$$

a ponieważ $(x - a)^k$ nie jest dzielnikiem zera w $P[x]$, więc $g = (x - a)h$, co jest sprzeczne z założeniem że $g(a) \neq 0$. □

Załóżmy, że P jest pierścieniem całkowitym i niezerowy wielomian $f \in P[x]$ ma parami różne pierwiastki $a_1, ..., a_m \in P$ o krotnościach odpowiednio $k_1, ..., k_m$. Z twierdzenia 3 wiemy, że wtedy $f = (x - a_1)^{k_1} g_1$ dla pewnego wielomianu $g_1 \in P[x]$, a zatem

$$0 = f(a_2) = (a_2 - a_1)^{k_1} g_1(a_2).$$

Ponieważ $a_2 \neq a_1$ i P jest pierścieniem całkowitym, więc $g_1(a_2) = 0$. Stąd a_2 jest pierwiastkiem wielomianu g_1, przy czym jego krotność jest równa k_2. Widzimy więc, że

$g_1 = (x-a_2)^{k_2}g_2$ dla pewnego $g_2 \in P[x]$, czyli $f = (x-a_1)^{k_1}(x-a_2)^{k_2}g_2$. Postępując dalej w ten sposób dochodzimy do wzoru

$$f = (x-a_1)^{k_1}(x-a_2)^{k_2}...(x-a_m)^{k_m}g$$

dla pewnego $g \in P[x]$. Ze wzoru tego wynika nierówność

$$k_1 + k_2 + ... + k_m \leqslant \operatorname{st} f. \tag{7}$$

Zatem liczba pierwiastków niezerowego wielomianu f liczonych wraz z ich krotnościami nie przekracza stopnia tego wielomianu.

Wniosek ten stosuje się w szczególności do pierścienia $\mathbb{Z}[x]$. Założenie, że P jest pierścieniem całkowitym jest tu istotne, co widać w następującym przykładzie.

Przykład 3. Niech $f = 2x^2+2x$. Rozpatrując ten wielomian w pierścieniu $\mathbb{Z}_4[x]$ widzimy, że $f(0) = f(1) = f(2) = f(3) = 0$. Zatem wielomian f stopnia 2 ma 4 pierwiastki. Funkcja wielomianowa f jest identyczna z funkcją zerową, chociaż f nie jest wielomianem zerowym.

Pochodną wielomianu $f = \sum_{i=0}^{n} a_i x^i \in P[x]$, gdzie $a_n \neq 0$ nazywamy wielomian

$$f' = a_1 + 2 \cdot a_2 x + ... + n \cdot a_n x^{n-1}.$$

Przypomnijmy, że dla $a \in P$, $k \in \mathbb{N}$ symbolem $k \cdot a$ oznaczamy sumę $a + ... + a$, gdzie liczba składników jest równa k. Dla uproszczenia będziemy także pisać krótko ka zamiast $k \cdot a$. Zamiast f' piszemy też $f^{(1)}$.

Uwaga 2. Jeżeli $\operatorname{char}(P)$ nie dzieli n, to $n \cdot a_n \neq 0$, a więc $\operatorname{st} f' = n-1 = \operatorname{st} f - 1$. Zatem gdy $\operatorname{char} P = 0$, to równość $\operatorname{st} f' = n - 1 = \operatorname{st} f - 1$ zachodzi dla każdego wielomianu $f \in P[x]$.

W przypadku, gdy $\operatorname{char}(P) = n$ i $\operatorname{st} f = n \geqslant 0$, mamy $\operatorname{st} f' < \operatorname{st} f - 1$.

Dla dowolnych wielomianów $f, g \in P[x]$ mamy

$$(f+g)' = f' + g', \quad (f \cdot g)' = f' \cdot g + f \cdot g'. \tag{8}$$

Twierdzenie 4. *Niech $a \in P$ będzie pierwiastkiem wielomianu $f \in P[x]$. Wówczas a jest pierwiastkiem wielokrotnym wtedy i tylko wtedy, gdy $f'(a) = 0$.*

Dowód. Załóżmy, że a jest pierwiastkiem wielokrotnym. Wtedy $f = (x-a)^k g$ dla pewnego $g \in P[x]$, gdzie $k > 1$. Wtedy

$$f' = k(x-a)^{k-1}g + (x-a)^k g',$$

więc $f'(a) = k(a-a)^{k-1}g(a) + (a-a)^k g'(a) = 0$, gdyż $k - 1 > 0$.

Załóżmy teraz, że a jest pierwiastkiem jednokrotnym. Wtedy $f = (x-a)g$ dla pewnego $g \in P[x]$ takiego, że $g(a) \neq 0$. Mamy

$$f' = g + (x-a)g',$$

więc $f'(a) = g(a) + (a-a)g'(a) = g(a) \neq 0$. Jeżeli więc $f'(a) = 0$, to a jest pierwiastkiem wielokrotnym. □

Jeśli $\operatorname{char}(P) = 0$, to krotność pierwiastka można wyznaczyć przy użyciu kolejnych pochodnych wielomianu. Dla $f \in P[x]$ pochodne wyższych rzędów definiujemy jako: $f^{(2)} = f'' = (f')'$, $f^{(3)} = (f^{(2)})'$ i ogólnie $f^{(k+1)} = (f^{(k)})'$ dla $k \in \mathbb{N}$.

Twierdzenie 5. *Niech* $\mathrm{char}(P) = 0$ *i* $a \in P$ *będzie pierwiastkiem wielomianu* $f \in P[x]$. *Jeżeli* $f^{(i)}(a) = 0$ *dla* $i = 1, 2, ..., k-1$ *i* $f^{(k)}(a) \neq 0$, *to pierwiastek* a *ma krotność* k.

Przykład 4. Niech $f(x) = x^3 - 5x^2 + 7x - 3 \in \mathbb{Z}[x]$. Mamy

$$f'(x) = 3x^2 - 10x + 7, \quad f''(x) = 6x - 10, \quad f^{(3)}(x) = 6,$$

więc $f(1) = f'(1) = 0$ i $f''(1) = -4 \neq 0$. Stąd 1 jest dwukrotnym pierwiastkiem f.

Pierwiastki ułamkowe

Twierdzenie 6. *Niech* P *będzie pierścieniem Gaussa i* $U(P)$ *będzie jego ciałem ułamków. Jeżeli wielomian*

$$f = a_0 + a_1 x + ... + a_n x^n \in P[x],$$

gdzie $a_n \neq 0$, *ma pierwiastek* $\frac{a}{b} \in U(P)$ *taki, że* a, b *są względnie pierwsze, to* $a \mid a_0$ *i* $b \mid a_n$.

Przykład 5. Niech $f = 3x^3 - x^2 + 3x - 1$. Jeśli $\frac{a}{b} \in \mathbb{Q}$ jest pierwiastkiem wielomianu f, przy czym $a, b \in \mathbb{Z}$ są względnie pierwsze, to $a \mid 1$, czyli $a = \pm 1$ i $b \mid 3$, czyli $b = \pm 1$ lub $b = \pm 3$. Zatem możliwe pierwiastki wymierne $\frac{a}{b}$ wielomianu f to: ± 1 i $\pm\frac{1}{3}$.

Mamy $f(1) = 4$, $f(-1) = -8$, $f\left(\frac{1}{3}\right) = 0$ i $f\left(-\frac{1}{3}\right) = -\frac{4}{9}$. Zatem jedynym wymiernym pierwiastkiem f jest $\frac{1}{3}$.

Rozkład wielomianów na czynniki nierozkładalne

Jeśli K jest ciałem, to $K[x]$ jest pierścieniem Gaussa. Zatem każdy wielomian $f \in K[x]$ taki, że $\mathrm{st}\, f > 0$ ma jednoznaczny rozkład na czynniki nierozkładalne.

Twierdzenie 7. *Niech* K *będzie ciałem i* $\mathrm{char}(K) = 0$. *Jeśli*

$$f = f_1^{k_1} f_2^{k_2} ... f_n^{k_n}$$

jest rozkładem wielomianu $f \in K[x]$ *na czynniki nierozkładalne, czyli* $f_1, f_2, ..., f_n \in K[x]$ *są nierozkładalne i* $f_i \not\sim f_j$ *dla* $i \neq j$ *oraz* $k_1, k_2, ..., k_n \in \mathbb{N}$, *to*

$$f' = f_1^{k_1 - 1} f_2^{k_2 - 1} ... f_n^{k_n - 1} g$$

dla pewnego $g \in K[x]$ *takiego, że* g *nie dzieli się przez żaden z wielomianów* $f_1, f_2, ..., f_n$.

Dowód. Niech $h = f_2^{k_2} ... f_n^{k_n}$. Wtedy $f = f_1^{k_1} h$, więc

$$f' = k_1 f_1^{k_1 - 1} f_1' h + f_1^{k_1} h' = f_1^{k_1 - 1} h_1,$$

gdzie $h_1 = k_1 f_1' h + f_1 h'$. Wielomian h_1 nie dzieli się przez f_1, gdyż w przeciwnym przypadku f_1 dzieliłby $f_1' h$. Ale f_1 nie dzieli h, więc dzieliłby f_1', co jest niemożliwe, gdyż $\mathrm{st}\, f_1' < \mathrm{st}\, f_1$.

Powtarzając to rozumowanie dla pozostałych wielomianów $f_2, ..., f_n$ stwierdzamy, że $f' = f_1^{k_1 - 1} f_2^{k_2 - 1} ... f_n^{k_n - 1} g$ i żaden z wielomianów $f_1, f_2, ..., f_n$ nie dzieli g. □

Wniosek 1. *Niech* K *będzie ciałem i* $\mathrm{char}(K) = 0$. *Jeśli*

$$f = f_1^{k_1} f_2^{k_2} ... f_n^{k_n}$$

jest rozkładem wielomianu $f \in K[x]$ *na czynniki nierozkładalne, to*

$$f_1^{k_1 - 1} f_2^{k_2 - 1} ... f_n^{k_n - 1} \sim \mathrm{NWD}(f, f').$$

Stąd

$$f/\operatorname{NWD}(f,f') \sim f_1 f_2 ... f_n,$$

czyli wielomian otrzymany przez podzielenie f przez $\operatorname{NWD}(f,f')$ ma te same czynniki w rozkładzie na wielomiany nierozkładalne, co f ale w pierwszej potędze.

Rozważmy szczególny przypadek, gdy czynniki w rozkładzie mają postać $x-a_i$, czyli f ma postać

$$f = a(x-a_1)^{k_1}(x-a_2)^{k_2}...(x-a_n)^{k_n},$$

a więc a_i jest pierwiastkiem wielomianu f o krotności k_i, $i=1,...,n$. Wtedy $f/\operatorname{NWD}(f,f')$ ma te same pierwiastki $a_1,a_2,...,a_n$, ale pojedyncze.

Niech P będzie pierścieniem Gaussa. Jak wiemy, dla dowolnych niezerowych elementów $a_1,a_2,...,a_n \in P$ istnieją $\operatorname{NWD}(a_1,a_2,...,a_n)$ i $\operatorname{NWW}(a_1,a_2,...,a_n)$. Elementy $a_1,a_2,...,a_n \in P$ są względnie pierwsze, gdy $1 \sim \operatorname{NWD}(a_1,a_2,...,a_n)$.

Niech K będzie ciałem ułamków pierścienia P. Jeżeli $f \in K[x]$, $f \neq 0$, to

$$f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n,$$

gdzie $a_0,...,a_n \in P$, $b_0,...,b_n \in P \setminus \{0\}$, $a_n \neq 0$ i $1 \sim \operatorname{NWD}(a_k,b_k)$, jeśli $a_k \neq 0$. ***Zawartością wielomianu*** f nazywamy element

$$c(f) = \frac{\operatorname{NWD}(a_0,...,a_n)}{\operatorname{NWW}(b_0,...,b_n)} \in K.$$

Jeżeli $f=0$, to przyjmujemy $c(f)=0$. Oczywiście zawartość $c(f)$ jest określona z dokładnością do stowarzyszenia.

Wielomian $g \in P[x]$ taki, że $c(g) \sim 1$ nazywamy ***wielomianem pierwotnym***. Oznacza to, że niezerowe współczynniki wielomianu g są względnie pierwsze. Dla dowolnego niezerowego wielomianu $f \in K[x]$ mamy $f = c(f)f_1$, gdzie $f_1 \in P[x]$ jest wielomianem pierwotnym.

Twierdzenie 8. *Niech K będzie ciałem ułamków pierścienia Gaussa P. Jeżeli wielomian $f \in P[x]$ jest nierozkładalny w $P[x]$, to f jest nierozkładalny w $K[x]$.*

W przypadku, gdy $f \in P[x]$ jest wielomianem pierwotnym, f jest nierozkładalny w $P[x]$ wtedy i tylko wtedy, gdy f jest nierozkładalny w $K[x]$.

Przykład 6. Wielomian $f = 2x^2 - 4$ ma jedynie pierwiastki niewymierne, więc jest nierozkładalny w $\mathbb{Q}[x]$. Jednak ma on rozkład $f = 2(x^2-2)$, który jest rozkładem właściwym w $\mathbb{Z}[x]$, gdyż 2 jest elementem nieodwracalnym w $\mathbb{Z}$. Nie jest to rozkład właściwy w $\mathbb{Q}[x]$, gdyż 2 jest odwracalne w $\mathbb{Q}$.

Twierdzenie 9. *Jeżeli P jest pierścieniem Gaussa, to $P[x]$ jest pierścieniem Gaussa. Elementami nierozkładalnymi w $P[x]$ są elementy nierozkładalne w pierścieniu P oraz wielomiany pierwotne, które są nierozkładalne w $K[x]$.*

Rozkład wielomianów na czynniki nierozkładalne w $\mathbb{C}[x]$ i $\mathbb{R}[x]$

Rozważmy pierścień wielomianów $\mathbb{C}[x]$ o współczynnikach zespolonych.

Twierdzenie 10 (zasadnicze twierdzenie algebry)**.** *Każdy wielomian $f \in \mathbb{C}[x]$ taki, że* $\operatorname{st} f \geqslant 1$ *ma co najmniej jeden pierwiastek zespolony.*

Wniosek 2. *Każdy wielomian $f \in \mathbb{C}[x]$ taki, że* $\operatorname{st} f \geqslant 1$ *można przedstawić w postaci*

$$f = a(x - z_1)^{k_1}(x - z_2)^{k_2}...(x - z_n)^{k_n}, \tag{9}$$

gdzie $a, z_1, z_2, ..., z_n \in \mathbb{C}[x]$ i $z_i \neq z_j$ dla $i \neq j$.

Oczywiście wielomian postaci $x - z_i$ jest nierozkładalny, więc (9) jest rozkładem f na czynniki nierozkładalne.

Niech teraz $f \in \mathbb{R}[x]$, $f = a_0 + a_1x + ... + a_nx^n$. Jeśli z jest zespolonym pierwiastkiem wielomianu f, to ponieważ $a_0, a_1, ..., a_n$ są liczbami rzeczywistymi, więc

$$0 = \overline{f(z)} = a_0 + a_1\overline{z} + ... + a_n\overline{z}^n,$$

czyli liczba sprzężona $\overline{z}$ jest również pierwiastkiem f. Wielomian f można rozłożyć na czynniki nierozkładalne w $\mathbb{C}[x]$ zgodnie ze wzorem (9), ale jeśli $z_i \in \mathbb{C} \setminus \mathbb{R}$, to istnieje j takie, że $z_j = \overline{z_i}$. Mamy

$$(x - z_i)(x - z_j) = (x - z_i)(x - \overline{z_i}) = x^2 - (z_i + \overline{z_i})x + z_i\overline{z_i} = x^2 - (2\operatorname{Re} z_i)x + |z_i|^2.$$

Jest to wielomian o współczynnikach rzeczywistych, który nie ma pierwiastków rzeczywistych, więc jest nierozkładalny w $\mathbb{R}[x]$.

Zatem wielomianami nierozkładalnymi w $\mathbb{R}[x]$ są wielomiany pierwszego stopnia i wielomiany drugiego stopnia bez pierwiastków rzeczywistych i łącząc w rozkładzie (9) pary postaci $(x-z_i)(x-\overline{z_i})$ otrzymujemy następujący rozkład wielomianu $f \in \mathbb{R}[x]$ na czynniki nierozkładalne:

$$f = a(x - a_1)^{k_1}(x - a_2)^{k_2}...(x - a_m)^{k_m} f_1^{l_1} f_2^{l_2} ... f_n^{l_n},$$

gdzie $a_1, a_2, ..., a_m \in \mathbb{R}$ są parami różnymi pierwiastkami wielomianu f, zaś $f_1, f_2, ..., f_n \in \mathbb{R}[x]$ są parami niestowarzyszonymi wielomianami drugiego stopnia bez pierwiastków rzeczywistych i $k_1, k_2, ..., k_m, l_1, l_2, ..., l_n \in \mathbb{N}$.

Kryteria nierozkładalności wielomianów

Omówimy kilka metod sprawdzania nierozkładalności wielomianów. Zacznijmy od najprostszego przypadku, gdy wielomian $f \in P[x]$ ma stopień 2 lub 3. Wtedy f może się rozkładać jedynie na iloczyn, w którym co najmniej jeden czynnik ma stopień 1. Jest to więc czynnik postaci $ax + b$. Wtedy $-b/a$ jest pierwiastkiem f w ciele ułamków K pierścienia P. Zatem jeśli f nie ma pierwiastka w K, to f jest nierozkładalny w $K[x]$. Jeśli dodatkowo f jest wielomianem pierwotnym, to f jest nierozkładalny także w $P[x]$. Dla sprawdzenie, czy f ma pierwiastki ułamkowe wystarczy użyć twierdzenia 6.

Twierdzenie 11 (kryterium Eisensteina). *Niech P będzie pierścieniem Gaussa i K będzie ciałem jego ułamków. Jeżeli dla wielomianu*

$$f = a_0 + a_1x + ... + a_nx^n \in P[x],$$

gdzie $a_n \neq 0$ istnieje element nierozkładalny $p \in P$ taki, że $p \mid a_i$ dla $i = 0, 1, ..., n-1$, p nie dzieli a_n i p^2 nie dzieli a_0, to f jest nierozkładalny w $K[x]$.

W pewnych przypadkach aby zastosować kryterium Eisensteina należy zmienić zmienna.

Przykład 7. Niech $f(x) = x^4 + 4x + 1$. Zastępujemy ten wielomian przez

$$f(x+1) = (x+1)^4 + 4(x+1) + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6$$

dla którego możemy zastosować kryterium Eisensteina z $p = 2$. Zatem wielomian $f(x+1)$ jest nierozkładalny w $\mathbb{Q}[x]$. Gdyby f nie był nierozkładalny w $\mathbb{Q}[x]$, to istniałby rozkład

$$f(x) = g(x)h(x),$$

gdzie $g, h \in \mathbb{Q}[x]$ są wielomianami stopnia mniejszego niż 4. Ale wtedy

$$f(x+1) = g(x+1)h(x+1),$$

co jest sprzeczne z nierozkładalnością wielomianu $f(x+1)$.