Geometria z algebrą liniową I

Arkadiusz Męcel

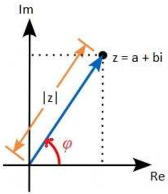
WYKŁAD 3, 19.10.2021 r.

Definicja 1.

Niech $z = a + bi$ będzie liczbą zespoloną. Liczbę rzeczywistą φ taką, że

$$z = |z|(\cos(\varphi) + i \cdot \sin(\varphi))$$

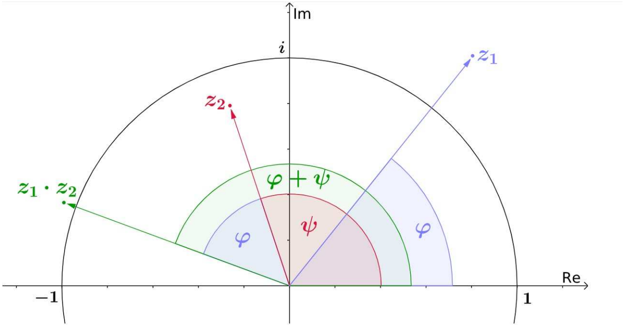
nazywamy **argumentem liczby zespolonej** z i oznaczamy $\arg(z)$.



Rys. 1. Płaszczyzna zespolona. Moduł i argument liczby zespolonej. Źródło: Wikipedia (z modyfikacjami).

Interpretacja geometryczna mnożenia liczb zespolonych. Dla niezerowych liczb zespolonych w, z zachodzą równości

$$\arg(z \cdot w) = \arg(z) + \arg(w), \quad |zw| = |z| \cdot |w|.$$

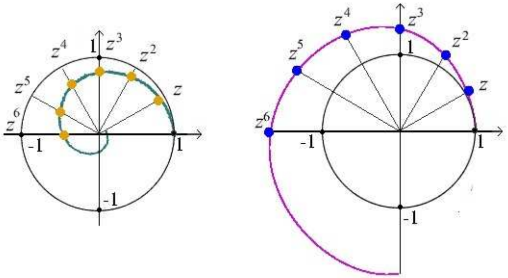


Rys. 2. Interpretacja geometryczna mnożenia liczb zespolonych.

Wzór Moivre'a

Niech $z = |z|(\cos\varphi + i \cdot \sin\varphi)$. Wówczas dla każdego n całkowitego dodatniego mamy:

$$z^n = |z|^n(\cos(n \cdot \varphi) + i \cdot \sin(n \cdot \varphi)).$$



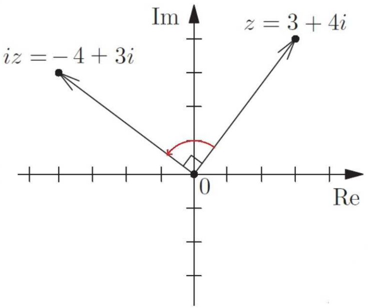
Rys. 3. Interpretacja geometryczna potęgowania liczb zespolonych. Źródło: http://www.suitcaseofdreams.net/.

Funkcje zmiennej zespolonej. Przykłady reprezentacji na płaszczyźnie.

Funkcja $f : \mathbb{C} \to \mathbb{C}$ zadana wzorem

$$f(z) = i \cdot z$$

to obrót płaszczyzny wokół zera o kąt $\frac{\pi}{2}$.



Rys. 4. Interpretacja geometryczna obrotu o kąt 90°. Źródło: Evan Chen (z modyfikacjami).

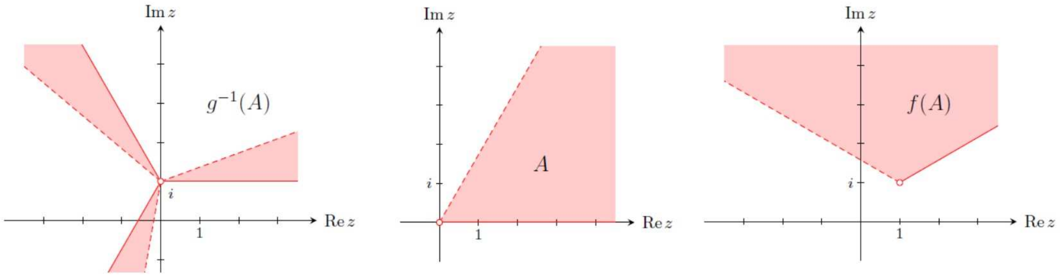
Funkcje zmiennej zespolonej. Przykłady reprezentacji na płaszczyźnie.

Obraz i przeciwobraz zbioru

$$A = \{z \in \mathbb{C} : z \neq 0, \arg z \in [0, \frac{\pi}{3})\}$$

przy funkcjach

$$f(z) = (1 + i\sqrt{3})z^2 + 1 + i, \quad g(z) = (z - i)^3.$$

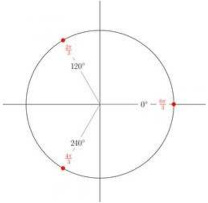


Rys. 5. Źródło: Ł. Kubat (z modyfikacjami).

Pierwiastki stopnia *n*-tego z zadanej liczby zespolonej

Stosując wzór Moivre'a $(|z|(\cos\varphi + i \cdot \sin\varphi))^n = |z|^n(\cos(n\varphi) + i \cdot \sin(n\varphi))$ widzimy, że są dokładnie 3 liczby zespolone, które podniesione do potęgi 3 dają 2:

$$\sqrt[3]{2}(\cos 0 + i \sin 0), \quad \sqrt[3]{2}(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}), \quad \sqrt[3]{2}(\cos\frac{4\pi}{3} + i \sin\frac{4\pi}{3}).$$



Rys. 6. Argumenty pierwiastków stopnia 3 z liczby 2 (o argumencie 0.

Uwaga-Definicja

Niech n będzie liczbą całkowitą dodatnią oraz $w = |w|(\cos\theta + i\sin\theta) \neq 0$. Wówczas liczby postaci:

$$\sqrt[n]{|w|}\left(\cos\frac{\theta+2\pi k}{n} + i\sin\frac{\theta+2\pi k}{n}\right), \qquad \text{dla } k = 0, 1, \ldots, n-1.$$

nazywamy **pierwiastkami stopnia n z w.**

W szczególności pierwiastki stopnia n z 1 to liczby:

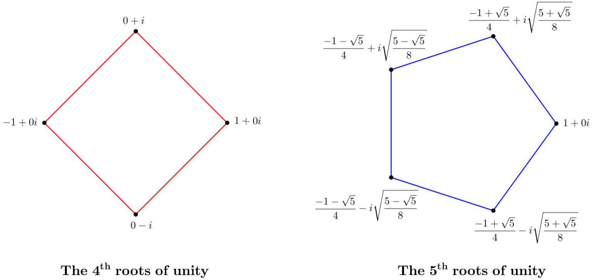
$$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \qquad \text{dla } k = 0, 1, \ldots, n-1.$$

Definicja 3.

Mówimy, że liczba $z \in \mathbb{C}$ jest **pierwiastkiem pierwotnym** stopnia n z 1, jeśli z jest pierwiastkiem stopnia n z 1, ale nie jest pierwiastkiem z 1 stopnia m, gdzie $m < n$.

Obserwacja geometryczna

Pierwiastki stopnia n z liczby zespolonej $w \neq 0$ są wierzchołkami n-kąta foremnego, np.



Rys. 7. Interpretacja geometryczna pierwiastków stopnia 4 i 5 z 1. Źródło: brilliant.org.

Definicja 4.

Wielomianem zmiennej x o współczynnikach w ciele K nazywamy wyrażenie:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

gdzie n jest dowolną liczbą całkowitą nieujemną oraz $a_0, a_1, \ldots, a_n \in K$.

Utożsamiamy przy tym takie napisy, jeśli różnią się o składniki postaci $0 \cdot x^i$ oraz jeśli różnią się kolejnością składników.

Elementy a_i nazywamy **współczynnikami** wielomianu. Zbiór wielomianów o współczynnikach z ciała K oznaczamy przez $K[x]$.

Stopniem wielomianu $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, ozn. $\deg(f)$, nazywamy

- największe takie i, że $a_i \neq 0$, jeśli istnieje
  i wtedy wyraz $a_{deg(f)}$ nazywamy **współczynnikiem wiodącym** wielomianu f,
- $-\infty$, jeśli $a_1 = a_2 = \ldots = a_n = 0$. Wtedy wielomian nazywamy **zerowym**.

Definicja 5.

Dla wielomianów

$$f = a_0 + a_1 x + \ldots + a_n x^n, \quad g = b_0 + b_1 x + \ldots + b_m x^m$$

ze zbioru $K[x]$ określamy:

- **sumę wielomianów** f oraz g:

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots,$$

- **wielomian przeciwny** do wielomianu f:

$$-f = (-a_0) + (-a_1)x + (-a_2)x^2 + \ldots,$$

- **iloczyn wielomianów** f oraz g:

$$f \cdot g = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

Stopień wielomianu, a działania dodawania i mnożenia

Niech K będzie ciałem oraz $0 \neq f, g \in K[x]$. Wówczas

$$\deg(f+g) \leq \max(\deg(f), \deg(g)), \quad \deg(f \cdot g) = \deg(f) + \deg(g).$$

Uwagi:

- Formuły te można naturalnie rozszerzyć na przypadek, gdy f lub g jest zerowy, przyjmując naturalne umowy odnośnie działań z użyciem $-\infty$.
- Równość w pierwszej nierówności zachodzi wtedy (ale nie tylko wtedy), gdy
$$\deg(f) \neq \deg(g).$$
- Jeśli K nie jest ciałem, wówczas tożsamość dla iloczynu trzeba zmodyfikować. Na przykład dla wielomianów f, g nad $\mathbb{Z}_4$ postaci:
$$f = 2x, \quad g = 1 + 2x$$
mamy $\deg(f) = \deg(g) = 1$, ale $\deg(fg) = 1$.

Definicja 6.

Niech $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ będzie wielomianem o współczynnikach w ciele K. Funkcję $f : K \to K$ daną wzorem

$$f(s) = a_0 + a_1 s + a_2 s^2 + \ldots + a_n s^n$$

nazwiemy **funkcją wielomianową** odpowiadającą wielomianowi f.

Pierwiastkami wielomianu f (inaczej: miejscami zerowymi) nazywamy wszystkie takie $s \in K$, że

$$f(s) = 0.$$

Przykłady.

- Funkcja $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ odpowiadająca $x^3 + 2x \in \mathbb{Z}_3[x]$ jest zerowa (znając wartości f. wielom. nie zawsze umiemy *rozpoznać* wielomian).
- Wielomian $w = x^2 + x + 1 \in \mathbb{R}[x]$ nie ma pierwiastków,
- Wielomian $w = x^2 + x + 1 \in \mathbb{C}[x]$ ma dwa pierwiastki.

Twierdzenie 1 (O dzieleniu z resztą).

Niech f, g będą wielomianami o współczynnikach z ciała K. Załóżmy ponadto, że g nie jest wielomianem zerowym. Wówczas istnieją wielomiany q i r takie, że:

$$f = q \cdot g + r, \quad \deg(r) < \deg(g). \qquad (*)$$

Ponadto wielomiany q, r są wyznaczone jednoznacznie.

Plan dowodu.

1. Wykażemy, że każdych $f, g \in K[x]$, gdzie $g \neq 0$ istnieją q, r takie, że $(*)$.
2. Wykażemy, że wielomiany q, r są wyznaczone jednoznacznie.

Dowód *istnienia* wielomianów q, r dla pary f, g.

- Jeśli $\deg(g) > \deg(f)$, to
$$f = 0 \cdot g + f.$$

- Jeśli $\deg(g) \leq \deg(f)$, to rozumowanie jest indukcją ze względu na stopień wielomianu f.

- Krok bazowy: $\deg(f) = 0$.

  Z założenia $g \neq 0$, więc $\deg(g) = 0$. Wtedy $\frac{f}{g} \in K$ oraz:
$$f = \frac{f}{g} \cdot g + 0.$$

- Krok indukcyjny. Niech $n = \deg(f)$ oraz $m = \deg(g) \leq n$ oraz
$$f = a_0 + a_1 x + \ldots + a_n x^n, \quad g = b_0 + b_1 x + \ldots + b_m x^m.$$

Dowód *istnienia* wielomianów q, r dla pary f, g, cd.

- Definiujemy wielomian $\tilde{f}$ stopnia $\leq n-1$ postaci:

$$\tilde{f} = b_m \cdot f - a_n x^{n-m} \cdot g = (b_m \cdot a_n x^n + \ldots) - (a_n b_m x^n + \ldots).$$

- Z założenia indukcyjnego istnieją wielomiany $\tilde{q}$ oraz $\tilde{r}$ takie, że

$$\tilde{f} = \tilde{q} \cdot g + \tilde{r}, \quad \text{gdzie} \quad \deg(g) > \deg(\tilde{r}).$$

- Z definicji $\tilde{f}$ mamy

$$b_m f - a_n x^{n-m} g = \tilde{q} \cdot g + \tilde{r}.$$

- Stąd wynika teza indukcji:

$$f = \left(\frac{a_n x^{n-m} + \tilde{q}}{b_m} \right) g + \frac{\tilde{r}}{b_m}.$$

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że
$$\deg(g) > \deg(r), \quad \deg(g) > \deg(r')$$
oraz
$$f = qg + r = q'g + r'.$$
- Zatem $(q - q')g = r' - r$.
- Jeśli $q \neq q'$, to $\deg(q - q')g \geq \deg(g)$.
- W rezultacie $\deg(r - r') \geq \deg(g)$.
- Mamy zatem sprzeczność, bo na mocy założenia o stopniach r, r' i g:
$$\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g)$$
- Zatem $q = q'$, co pociąga za sobą $r = r'$.

Twierdzenie 2 (Bezout).

Niech $f \in K[x]$, gdzie K jest ciałem. Następujące warunki są równoważne.

1. Element $s \in K$ jest pierwiastkiem wielomianu f.
2. Istnieje $g \in K[x]$ taki, że $f = (x - s)g$.

Dowód:

- Niech s będzie pierwiastkiem wielomianu f. Zgodnie z Twierdzeniem 1 istnieją wielomiany q, r takie, że
$$f = q(x - s) + r,$$
gdzie $\deg(r) < \deg(g) = 1$. A zatem r jest wielomianem stałym.
- Skoro s jest pierwiastkiem f, to $0 = f(s) = (s - s)q(s) + r(s) \Rightarrow 0 = r(s)$. Skoro r jest wielomianem stopnia 0, to $r = 0$. A zatem (1) implikuje (2).
- Jeśli $f = (x - s)g$, dla pewnego $g \in K[x]$, to $f(s) = (s - s)g(s) = 0$, co daje drugą implikację.

Rozkład wielomianu na czynniki, a istnienie pierwiastka.

Przypomnienie

Niech K będzie ciałem i niech $a, b \in K$. Wówczas jeśli $ab = 0$, to $a = 0$ lub $b = 0$.

Wniosek z definicji pierwiastka

Niech K będzie ciałem. Jeśli $s \in K$ jest pierwiastkiem niezerowego wielomianu $f \in K[x]$, to nie istnieją takie $g, h \in K[x]$, że:

- s nie jest pierwiastkiem ani g, ani h,
- $f = gh$.

Oczywiście istnieją rozkłady wielomianów na niestałe czynniki (i to jednoznaczne – co nie jest oczywiste), które nie mają pierwiastków. Np. nad $\mathbb{Q}$ mamy:

$$x^4 + 4 = (x^2 + 2)^2 - (2x)^2 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Przykładowe wnioski z twierdzenia Bezout.

- Jeśli $s \in K$ nie jest pierwiastkiem wielomianów $f, g \in K[x]$ oraz dla pewnych m, n całkowitych dodatnich mamy:
$$(x-s)^m \cdot f = (x-s)^n \cdot g,$$
to $m = n$ oraz $f = g$.
- Jeśli $s \in K$ nie jest pierwiastkiem wielomianu $g \in K[x]$ oraz dla pewnego $f \in K[x]$ oraz całkowitego dodatniego r mamy:
$$f = (x-s)^r \cdot g,$$
to wielomian f ma o r pierwiastków więcej niż wielomian g.
- Niech $f \in K[x]$, gdzie $\deg(f) = n \geq 0$. Wówczas f ma co najwyżej n pierwiastków. Co więcej, jeśli f rozkłada się na iloczyn czynników stopnia 1 (liniowych), to rozkład ten jest jednoznaczny z dokładnością do kolejności czynników i wyrazu wiodącego.

Wniosek.

Niech $f \in K[x]$, gdzie $\deg(f) = n \geq 0$. Wówczas f ma co najwyżej n pierwiastków. Co więcej, jeśli f rozkłada się na iloczyn czynników liniowych, to rozkład ten jest jednoznaczny z dokładnością do kolejności czynników i wyrazu wiodącego.

Definicja 7.

Jeśli każdy wielomian stopnia większego od 0 o współczynnikach z ciała K ma w ciele K pierwiastek, to K nazywamy **ciałem algebraicznie domkniętym**.

Twierdzenie 3.

Niech K będzie ciałem. Następujące warunki są równoważne.

1. Ciało K jest algebraicznie domknięte.
2. Każdy wielomian stopnia > 0 o współczynnikach z K rozkłada się nad K na czynniki stopnia 1 (to znaczy: jest iloczynem wielomianów stopnia 1 o współczynnikach z K).

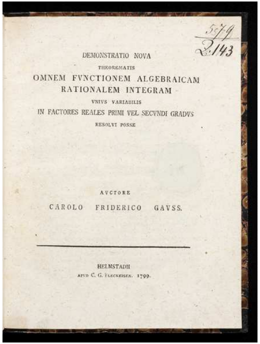
Dowód.

- Załóżmy, że K jest ciałem algebraicznie domkniętym. Pokażemy, że każdy wielomian stopnia > 0 rozkłada się nad K na współczynniki liniowe. Krok bazowy indukcji jest jasny.
- Załóżmy prawdziwość naszego założenia dla wielomianów stopnia $n - 1$. Niech f będzie wielomianem stopnia n.
- Ciało K jest algebraicznie domknięte, więc f ma pierwiastek $c \in K$. Stąd $f(x) = (x - c) \cdot g(x)$, dla pewnego wielomianu $g \in K[x]$, na mocy tw. Bezout.
- Wielomian g jest zatem stopnia $n - 1$, więc z założenia indukcyjnego g jest iloczynem czynników stopnia 1 o współczynnikach z K. Stąd f jest iloczynem czynników stopnia 1 o współczynnikach z K.
- Na odwrót: jeśli f jest iloczynem wielomianów stopnia 1 o współczynnikach w K, to każdy taki czynnik stopnia 1 ma pierwiastek w K, będący też pierwiastkiem wielomianu f. A zatem (2) implikuje (1).

Zasadnicze Twierdzenie Algebry (Gauss, 1799)

Ciało $\mathbb{C}$ jest algebraicznie domknięte.

W przyszłości poznacie Państwo kilka dowodów.


DEMONSTRATIO NOVA
THEOREMATIS
OMNEM FVNCTIONEM ALGEBRAICAM
RATIONALEM INTEGRAM
VNIVS VARIABILIS
IN FACTORES REALES PRIMI VEL SECVNDI GRADVS
RESOLVI POSSE

AVCTORE
CAROLO FRIDERICO GAVSS.

HELMSTADII
APVD C. G. FLECKEISEN. 1799.

Rys. 8. Pierwsza strona doktoratu Gaussa zawierającego (nie do końca poprawny) dowód Zasadniczego Twierdzenia Algebry.

Wniosek

Każdy wielomian $w \in \mathbb{R}[x]$ stopnia większego od 0 rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.

Szkic dowodu.

- Przypomnijmy: dla $z_1, z_2 \in \mathbb{C}$ mamy $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ oraz $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.
- Jeśli $s \in \mathbb{C}$ jest pierwiastkiem wielomianu $w = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$, to również $\overline{s}$ jest pierwiastkiem tego wielomianu. Istotnie,

$$\begin{aligned} 0 = \overline{0} &= \overline{a_n s^n + \ldots + a_1 s + a_0} = \\ &= \overline{a_n}\,\overline{s^n} + \ldots + \overline{a_1 s} + \overline{a_0} = \\ &= a_n (\overline{s})^n + \ldots + a_1 \overline{s} + a_0. \end{aligned}$$

- Indukcja ze względu na stopień w. Dla $\deg(w) = 1$ oczywiste.
- Jeśli $r_0 \in \mathbb{R}$ jest pierwiastkiem w, to $w = (x - r_0)g$, gdzie $g \in \mathbb{R}[x]$.
- Jeśli $z_0 \notin \mathbb{R}$ i $\overline{z_0}$ to pierwiastki w, wówczas $(x - z_0)(x - \overline{z_0}) \in \mathbb{R}[x]$ dzieli w.

Twierdzenie (Wzory Viete'a)

Niech $x_1, x_2, x_3, \ldots, x_n$ będą pierwiastkami wielomianu $a_n x^n + \ldots + a_1 x + a_0$, gdzie $a_n \neq 0$. Wówczas zachodzą równości:

$$\begin{cases} x_1 + x_2 + \ldots + x_n = \frac{-a_{n-1}}{a_n} \\ x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ x_1x_2x_3 \ldots x_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

Dowód:

- Indukcja ze względu na n. Dla n=1 dowód jest oczywisty. Załóżmy, że dla każdego wielomianu stopnia n, wzory te są prawdziwe. Rozważmy wielomian stopnia n+1, o pierwiastkach: $x_1, x_2, x_3, \ldots, x_n, x_{n+1}$. Zgodnie z twierdzeniem Bezout istnieje wielomian g(x) (którego wiodący współczynnik to 1), taki, że:

$$f(x) = a_{n+1} \cdot (x - x_1) \cdot g(x).$$

Twierdzenie (Wzory Viete'a)

Niech $x_1, x_2, x_3, \ldots, x_n$ będą pierwiastkami wielomianu $a_n x^n + \ldots + a_1 x + a_0$, gdzie $a_n \neq 0$. Wówczas zachodzą równości:

$$\begin{cases} x_1 + x_2 + \ldots + x_n = \frac{-a_{n-1}}{a_n} \\ x_1 x_2 + x_1 x_3 + \ldots + x_1 x_n + x_2 x_3 + \ldots + x_2 x_n + \ldots + x_{n-1} x_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ x_1 x_2 x_3 \ldots x_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

Dowód cd.:

- Wielomian g jest stopnia n, i jego pierwiastkami są $x_2, x_3, \ldots, x_n, x_{n+1}$.Więcej pierwiastków, zgodnie z udowodnionym wcześniej faktem, mieć nie może. Zatem są to jego wszystkie pierwiastki. Z założenia indukcyjnego mamy:

  $$g(x) = x^n - (x_2 + x_3 + \ldots + x_{n+1})x^{n-1} + \ldots + (-1)^{n+1}(x_2 x_3 \ldots x_{n+1}).$$

  Wymnażając g w takiej postaci przez $a_{n+1} \cdot (x - x_1)$ dostajemy tezę.