

Algebra dla MSEM 1, 2019/2020

ćwiczenia 13. – rozwiązania

15 listopada 2019

1. Sprawdź, że $p \in \mathbb{N} \setminus \{0, 1\}$ jest liczbą pierwszą wtedy i tylko wtedy, gdy $\mathbb{Z}_p$ jest ciałem.

Założmy, że p jest liczbą pierwszą. Jedyną nieoczywistą rzeczą jest istnienie odwrotności. Ale jeśli $a \in \mathbb{Z}_p$ i $a \neq 0$ to a i p są względnie pierwsze, więc z Małego Twierdzenia Fermata a^{p-1} dzieli się przez p z resztą 1. A zatem $a \cdot a^{p-2} = 1$ w $\mathbb{Z}_p$.

Jeśli natomiast $p = ab$, gdzie $a, b \neq 1$ oraz $a, b > 0$, to $ab = 0$ w $\mathbb{Z}_p$. Założmy dążąc do sprzeczności, że $\mathbb{Z}_p$ jest ciałem. Wtedy istnieje a^{-1} , a więc $a^{-1}ab = 1 \cdot b = b$ z jednej strony ale $a^{-1}ab = a^{-1} \cdot 0 = 0$ z drugiej. Zatem $b = 0$ wbrew założeniu.

2. Niech K będzie ciałem oraz $a, b, c \in K$. Wykaż, że

- (a) jeśli $a + c = b + c$, to $a = b$.

Skoro K jest ciałem to istnieje $-c$. Korzystając z łączności dodawania oraz własności zera mamy więc:

$$a = a + 0 = a + (c + (-c)) = (a + c) + (-c) = (b + c) + (-c) = b + (c + (-c)) = b + 0 = b.$$

- (b) jeśli $ac = bc$ oraz $c \neq 0$, to $a = b$.

Skoro K jest ciałem to istnieje c^{-1} . Korzystając z łączności mnożenia oraz własności jedynki mamy więc:

$$a = a \cdot 1 = a \cdot (c \cdot c^{-1}) = (a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1} = b \cdot (c \cdot c^{-1}) = b \cdot 1 = b.$$

- (c) $a \cdot 0 = 0$ oraz $(-1) \cdot a = -a$.

Zauważmy, że $a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a \cdot (0 + 1) = a \cdot 1 = a = 0 + a$, a zatem na mocy pierwszej z udowodnionych tożsamości mamy $a \cdot 0 = 0$.

A zatem $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0 = -a + a$, a zatem znów na mocy pierwszej z udowodnionych tożsamości mamy $(-1) \cdot a = -a$.

3. W $\mathbb{Z}_5$ znaleźć:

- (a) -3 oraz 4^{-1} ,

W $\mathbb{Z}_5$ $-3 = 2$, bowiem $3 + 2 = 0$. $4^{-1} = 4$, bowiem $4 \cdot 4 = 1$ (w $\mathbb{Z}$ $4 \cdot 4 = 16$, dzieli się przez 5 z resztą 1).

- (b) wszystkie rozwiązania równania $2x^2 + 3 = 0$

A zatem $x^2 = -3 \cdot 2^{-1} = 2 \cdot 3 = 1$, a liczbami o tej własności w $\mathbb{Z}_5$ są 1 oraz 4.

- (c) wszystkie rozwiązania równania $x^5 - 1 = 0$.

A zatem $x^5 = 1$. Mamy $1^5 = 1$, $2^5 = 2$, $3^5 = 3$ oraz $4^5 = 4$ (jeśli ktoś nie chce liczyć może skorzystać z Małego Twierdzenia Fermata). A zatem jedyną taką liczbą jest 1.

4. Skonstruuj ciało złożone z 4 elementów.

Istnieje cztero-elementowe ciało $\{0, 1, a, a + 1\}$ w którym operacje działają w następujący sposób:

+	0	1	a	a + 1
0	0	1	a	a + 1
1	1	0	a + 1	a
a	a	a + 1	0	1
a + 1	a + 1	a	1	0

$\cdot$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

5. Niech $a, b, c \in \mathbb{C}$ oraz $a \neq 0$. Niech $d \in \mathbb{C}$ będzie liczbą taką, że $d^2 = b^2 - 4ac$. Wykazać, że pierwiastkami wielomianu $ax^2 + bx + c \in \mathbb{C}[x]$ są liczby $\frac{-b+d}{2a}$ oraz $\frac{-b-d}{2a}$.

Rzeczywiście,

$$\begin{aligned} a(-b+d/2a)^2 + b(-b+d/2a) + c &= b^2/4a - bd/2a + d^2/4a - b^2/2a + bd/2a + c = (b^2 - 4ac)/4a - b^2/4a + c = \\ &= b^2/4a - c - b^2/4a + c = 0 \end{aligned}$$

oraz

$$\begin{aligned} a(-b-d/2a)^2 + b(-b-d/2a) + c &= b^2/4a + bd/2a + d^2/4a - b^2/2a - bd/2a + c = (b^2 - 4ac)/4a - b^2/4a + c = \\ &= b^2/4a - c - b^2/4a + c = 0. \end{aligned}$$

6. Niech $f \in \mathbb{R}[x]$. Wykazać, że:

- (a) jeśli $c \in \mathbb{C}$ jest pierwiastkiem wielomianu f w $\mathbb{C}$, to $\bar{c}$ też jest pierwiastkiem f ,

Niech $c = a \cdot (\cos \phi + i \sin \phi)$, $a, \phi \in \mathbb{R}$. Niech $f = a_0 + a_1x + \dots + a_nx^n$, $a_0, \dots, a_n \in \mathbb{R}$. W takim razie:

$$0 = f(c) = a_0 + a_1c + \dots + a_nc^n = a_0 + a_1a(\cos \phi + i \sin \phi) + a_2a^2(\cos 2\phi + i \sin 2\phi) + \dots + a_na^n(\cos n\phi + i \sin n\phi),$$

Zatem

$$0 = a_1ai \sin \phi + a_2a^2i \sin 2\phi + \dots + a_na^n i \sin n\phi = -(a_1ai \sin(-\phi) + a_2a^2i \sin(-2\phi) + \dots + a_na^n i \sin(-n\phi)),$$

Zatem

$$\begin{aligned} 0 = f(c) &= a_0 + a_1a(\cos(-\phi) + i \sin(-\phi)) + a_2a^2(\cos(-2\phi) + i \sin(-2\phi)) + \dots + a_na^n(\cos(-n\phi) + i \sin(-n\phi)) = \\ &= f(\bar{c}), \end{aligned}$$

czyli $\bar{c}$ to też pierwiastek.

- (b) wielomian f rozkłada się nad $\mathbb{R}$ na czynniki stopnia ≤ 2 .

Na podstawie poprzedniego punktu wystarczy zauważyć, że

$$(x-c)(x-\bar{c}) = x^2 - (c+\bar{c})x + c\bar{c} = x^2 - 2\Re(c)x + |c|^2 \in \mathbb{R}[x].$$

7. Dla każdego z poniższych wielomianów znaleźć wszystkie jego pierwiastki, rozłożyć ten wielomian nad $\mathbb{C}$ na czynniki stopnia 1 oraz rozłożyć go nad $\mathbb{R}$ na czynniki stopnia ≤ 2 .

- (a) $x^2 + 4x + 5$,

$\Delta = 16 - 20 = -4$, $d = 2i$, więc mamy pierwiastki $-2-i$ oraz $-2+i$, czyli $x^2 + 4x + 5 = (x+2+i)(x+2-i)$ w liczbach zespolonych. To już jest wielomian stopnia ≤ 2 , jeśli chodzi o jego rozkład w liczbach rzeczywistych.

- (b) $x^4 - 2x^2 + 4$,

Niech $z = x^2$, wtedy mamy wielomian $z^2 - 2z + 4 = 0$. $\Delta = 4 - 16 = -12$, $d = 2i\sqrt{3}$, zatem ten wielomian się zeruje w $z \in \{1-i\sqrt{3}, 1+i\sqrt{3}\}$, czyli dla $x \in \{\sqrt{6}/2 + i\sqrt{2}/2, -\sqrt{6}/2 + i\sqrt{2}/2, \sqrt{6}/2 - i\sqrt{2}/2, -\sqrt{6}/2 - i\sqrt{2}/2\}$, czyli

$$x^4 - 2x^2 + 4 = (x - \sqrt{6}/2 - i\sqrt{2}/2)(x - \sqrt{6}/2 + i\sqrt{2}/2)(x + \sqrt{6}/2 - i\sqrt{2}/2)(x + \sqrt{6}/2 + i\sqrt{2}/2)$$

czyli w liczbach rzeczywistych rozkłada się na:

$$x^4 - 2x^2 + 4 = (x^2 - 2\sqrt{6}x + 2)(x^2 + 2\sqrt{6}x + 2).$$

(c) $x^7 - x$.

Mamy $x^7 - x = x(x^6 - 1)$, a zatem pierwiastki to 0 oraz pierwiastki szóstego stopnia z 1, czyli $1, 1/2 + i\sqrt{3}/2, -1/2 + i\sqrt{3}/2, -1, -1/2 - i\sqrt{3}/2, 1/2 - i\sqrt{3}/2$, a zatem:

$$x^7 - x = x(x-1)(x-1/2-i\sqrt{3}/2)(x+1/2-i\sqrt{3}/2)(x+1)(x+1/2+i\sqrt{3}/2)(x-1/2+i\sqrt{3}/2)$$

co w rozkładzie w liczbach rzeczywistych daje:

$$x^7 - x = x(x-1)(x+1)(x^2-x+1)(x^2+x+1).$$

8. Niech K będzie ciałem. Wykazać, że:

- (a) Wielomian stopnia n o współczynnikach w K może mieć w K co najwyżej n różnych pierwiastków. Dowiedzimy indukcyjnie. Rzeczywiście, dla $n = 0$ teza jest oczywista. Załóżmy zatem, że dla $n - 1$ zachodzi badana teza, oraz że f jest wielomianem stopnia n oraz $a \in K$ jest jego pierwiastkiem. Wobec tego $f(x) = (x - a)g(x)$ dla pewnego wielomianu stopnia $n - 1$. $f(x) = 0$ wtedy i tylko wtedy, gdy $x = a$ lub gdy $g(x) = 0$, ale g na mocy założenia indukcyjnego ma co najwyżej $n - 1$ pierwiastków.
- (b) Przekształcenie $K[x] \rightarrow K^K$ przypisujące każdemu wielomianowi odpowiadającą mu funkcję wielomianową jest różnowartościowe wtedy i tylko wtedy, gdy K jest ciałem nieskończonym. Zauważmy, że jeśli $K = \{0, a_1, \dots, a_n\}$ jest ciałem skończonym to dla każdego $1 \leq i \leq n$ istnieje $p_i \in \mathbb{N}$, że $a_i^{p_i} = 1$. Zatem wielomian

$$f(x) = x(x^{p_1} - 1)(x^{p_2} - 1) \cdot \dots \cdot (x^{p_n} - 1)$$

ma tę cechę, że $f(x) = 0$ dla każdego $x \in K$, a zatem ma tę samą funkcję wielomianową, co wielomian 0, będąc od niego różnym.

Zauważmy również, że jeśli K jest nieskończone oraz $f(x) = 0$ dla pewnego wielomianu $f \in K[x]$ oraz każdego $x \in K$, to $f = 0$. Załóżmy, że $f \neq 0$ dążąc do sprzeczności, którą osiągamy od razu jeśli stopień wielomianu jest równy 0. Jeśli natomiast stopień f jest równy $n > 0$, to ponieważ dla każdego $x \in K$ $f(x) = 0$, mamy że

$$f(x) = a(x - x_1) \cdot \dots \cdot (x - x_n),$$

dla pewnych $a \in K \setminus \{0\}$ oraz $x_1, \dots, x_n \in K$. Ale istnieje $b \in K \setminus \{x_1, \dots, x_n\}$ i wstawiając b do powyższego wyrażenia otrzymujemy sprzeczność.

Zatem założmy przeciwnie, że istnieją różne $f, g \in K[x]$, mające te same funkcje. Wtedy $f - g \in K[x]$ będzie wielomianem różnym od 0, takim że dla każdego $x \in K$, $(f - g)(x) = 0$, co daje sprzeczność.