

Geometria z algebrą liniową, 2019/2020

ćwiczenia 3. – rozwiązania

10 lub 11 października 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. Jediną 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. Niech K będzie ciałem oraz L będzie podciałem ciała K . Wykaż, że

- (a) jeśli $K = \mathbb{R}$, to $\mathbb{Q} \subseteq L$.

Ponieważ $1 \in L$, to dla każdej liczby $n \in \mathbb{N} \setminus \{0\}$ mamy $n = 1 + \dots + 1 \in L$ (dowód indukcyjny). W takim razie także $-n \in L$, czyli $\mathbb{Z} \subseteq L$. Wobec tego dla każdego $q \in \mathbb{Z} \setminus \{0\}$, $1/q \in L$, czyli też dla każdego $p \in \mathbb{Z}$, $p/q \in L$. Wobec tego $\mathbb{Q} \subseteq L$.

- (b) jeśli $K = \mathbb{R}$ oraz $\sqrt{2} \in L$, to $\mathbb{Q}(\sqrt{2}) \subseteq L$.

Wiemy już, że $\mathbb{Q} \subseteq L$. Ale skoro $\sqrt{2} \in L$ to dla każdego $q \in \mathbb{Q}$, $q\sqrt{2} \in L$. Wobec tego dla każdych $p, q \in \mathbb{Q}$, $p + q\sqrt{2} \in L$, czyli $\mathbb{Q}(\sqrt{2}) \subseteq L$.

- (c) jeśli $K = \mathbb{Q}$ to $L = \mathbb{Q}$.

Rozumowanie z pierwszego podpunktu prowadzi do wniosku, że $\mathbb{Q} \subseteq L$, ale $L \subseteq K = \mathbb{Q}$, więc $L = \mathbb{Q}$.

- (d) jeśli $K = \mathbb{Z}_p$, to $L = \mathbb{Z}_p$.

Skoro $1 \in L$, to dla każdego $a \in \mathbb{Z}_p \setminus \{0\}$, $a = 1 + \dots + 1 \in L$.

4. ($\cdot$) 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.

5. $(\cdot)$ Dla których liczb $p = 2, 3, 5, 7$ ciąg $(1, 1, 1, 1)$ jest rozwiązaniem następującego układu równań w $\mathbb{Z}_p$?

$$\begin{cases} x + y + t = 0 \\ y - z + t = 1 \\ x + y + z = 0 \end{cases}$$

Sprawdzamy:

(a) dla $p = 2$, $1 + 1 + 1 = 1$, więc nie jest spełnione pierwsze równanie

(b) dla $p = 3$, $1 + 1 + 1 = 0$, $1 - 1 + 1 = 1$ oraz $1 + 1 + 1 = 0$, więc $(1, 1, 1, 1)$ jest rozwiązaniem

(c) dla $p = 5$ oraz $p = 7$, $1 + 1 + 1 = 3$, czyli nie jest spełnione pierwsze równanie

6. Znaleźć rozwiązanie ogólne następującego układu równań o współczynnikach w $\mathbb{Z}_5$.

$$\begin{cases} 2x + 3y + z + 4t = 1 \\ 3x + y + 2z + 4t = 2 \\ 3x + 3y + z + 3t = 1 \end{cases}$$

Zapisujemy macierz w kolejności z, x, y, t i sprowadzamy do postaci schodkowej

$$\left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 2 & 3 & 1 & 4 & 2 \\ 1 & 3 & 3 & 3 & 1 \end{array} \right] \xrightarrow{w_2 - 2w_1, w_3 - w_1} \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & 4 & 0 & 1 & 0 \\ 0 & 1 & 0 & 4 & 0 \end{array} \right] \xrightarrow{w_3 + w_2, w_1 + 2w_2} \left[\begin{array}{cccc|c} 1 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \xrightarrow{w_2 \cdot 4} \left[\begin{array}{cccc|c} 1 & 0 & 3 & 1 & 1 \\ 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

A zatem mamy

$$\begin{cases} z = 1 + 2y + 4t \\ x = t \end{cases}$$

Co w postaci parametrycznej daje $(t, y, 1 + 2y + 4t, t)$, $y, t \in \mathbb{Z}_5$.

7. 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

·	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

8. $(\star)$ Rozstrzygnij czy istnieją ciała zawierające dokładnie 6 i 8 elementów.

Nie istnieje ciało 6-cio elementowe. Załóżmy przeciwnie, że K ma 6 elementów. Rzędem elementu $a \in K$ nazwiemy najmniejszą liczbę n taką, że suma n elementów a daje 0. Dojście do sprzeczności przebiega w następujących krokach.

- (a) Nie istnieje element o rzędzie 4. Załóżmy przeciwnie, że istnieje taki element a . Wtedy $0, a, a + a$ i $a + a + a$ to różne elementy. Zatem jest jakiś inny element b , ale $a + b$ też jest inny od tych elementów i od b , co łatwo udowodnić, np. jeśli $a + b = a + a + b$, to $a = 0$, a tak nie jest. Ale także $a + a + b$ jest różne od dotychczasowych elementów, co znów łatwo się dowodzi, np. jeśli $a + a + b = 0 = a + a + a + s$, to $b = a + a$, a to nieprawda. Zatem mamy różne elementy: $0, a, a + a, a + a + a, b, a + b, a + a + b -$ ale to w sumie 7, a elementów ma być 6.
- (b) Dokładnie analogicznie pokazujemy, że nie istnieje element o rzędzie 5.
- (c) Nie istnieją też dwa elementy o rzędzie 2. Załóżmy bowiem przeciwnie, że są takie elementy a i b . Wobec tego $a + b \neq 0$, bo jeśli $a + b = 0 = a + a$, to $a = b$, a tak ma nie być. Zatem $0, a, b$ i $a + b$ to cztery różne elementy. Weźmy zatem kolejny inny element c . Podobnie jak poprzednio dowodzimy, że $a + c$ i $b + c$ to jeszcze inne i inne od siebie elementy – znów jest więc 7 różnych rzeczy, a jest 6.
- (d) Jest parzysta liczba elementów o rzędzie 3. Rzeczywiście, jeśli a jest rzędu 3, to również $a + a$ jest rzędu 3, bo $(a + a) + (a + a) = a \neq 0$, a $(a + a) + (a + a) + (a + a) = 0$.
- (e) Zatem istnieje element rzędu 6. Załóżmy przeciwnie, że nie ma takiego elementu. Zatem mamy 5 niezerowych elementów i muszą być one rzędu 2 lub 3. Skoro jest maksimum jeden element rzędu 2, to istnieje element rzędu 3, nazwijmy go b . Skoro elementów rzędu 3 jest parzyście wiele, to istnieje element rzędu 2, nazwijmy go a . Ale w takim razie $a + b \neq 0$, bo w przeciwnym przypadku $a + b = a + a$, więc $a = b$, sprzeczność. Ale też $(a + b) + (a + b) = b + b \neq 0$ oraz $(a + b) + (a + b) + (a + b) = a \neq 0$. W takim razie element $a + b$ nie jest rzędu ani 2, ani 3, sprzeczność.
- (f) W takim razie niech a będzie istniejącym elementem o rzędzie 6. W takim razie $K = \{0, a, a + a, a + a + a, a + a + a + a, a + a + a + a + a\}$. Ale w takim razie dla każdego $c \in K$, $c + c + c + c + c + c = 0$. Niech $a \cdot b = i \in K$. Zatem $(a + a) \cdot (a + a + a) = (a \cdot a) + (a \cdot a) + (a \cdot a) + (a \cdot a) + (a \cdot a) + (a \cdot a) = i + i + i + i + i + i = 0$, a zatem $a + a = 0$ lub $a + a + a = 0$, ale to sprzeczność, bo a jest rzędu 6.

Istnieje ośmio-elementowe ciało $\{0, 1, a, a + 1, a^2, a^2 + 1, a^2 + a, a^2 + a + 1\}$ w którym operacje działają w następujący sposób:

+	0	1	a	$a + 1$	a^2	$a^2 + 1$	$a^2 + a$	$a^2 + a + 1$
0	0	1	a	$a + 1$	a^2	$a^2 + 1$	$a^2 + a$	$a^2 + a + 1$
1	1	0	$a + 1$	a	$a^2 + 1$	a^2	$a^2 + a + 1$	$a^2 + a$
a	a	$a + 1$	0	1	$a^2 + a$	$a^2 + a + 1$	a^2	$a^2 + 1$
$a + 1$	$a + 1$	a	1	0	$a^2 + a + 1$	$a^2 + a$	$a^2 + 1$	a^2
a^2	a^2	$a^2 + 1$	$a^2 + a$	$a^2 + a + 1$	0	1	a	$a + 1$
$a^2 + 1$	$a^2 + 1$	a^2	$a^2 + a + 1$	a^2	1	0	$a + 1$	a
$a^2 + a$	$a^2 + a$	$a^2 + a + 1$	a^2	$a^2 + 1$	a	$a + 1$	0	1
$a^2 + a + 1$	$a^2 + a + 1$	$a^2 + a$	$a^2 + 1$	a^2	$a + 1$	a	1	0

·	0	1	a	$a + 1$	a^2	$a^2 + 1$	$a^2 + a$	$a^2 + a + 1$
0	0	0	0	0	0	0	0	0
1	0	1	a	$a + 1$	a^2	$a^2 + 1$	$a^2 + a$	$a^2 + a + 1$
a	0	a	a^2	$a^2 + a$	$a + 1$	1	$a^2 + a + 1$	$a^2 + 1$
$a + 1$	0	$a + 1$	$a^2 + a$	$a^2 + 1$	$a^2 + a + 1$	a^2	1	a
a^2	0	a^2	$a + 1$	$a^2 + a + 1$	$a^2 + a$	a	$a^2 + 1$	1
$a^2 + 1$	0	$a^2 + 1$	1	a^2	a	$a^2 + a + 1$	$a + 1$	$a^2 + a$
$a^2 + a$	0	$a^2 + a$	$a^2 + a + 1$	1	$a^2 + 1$	$a + 1$	a	a^2
$a^2 + a + 1$	0	$a^2 + a + 1$	$a^2 + 1$	a	1	$a^2 + a$	a^2	$a + 1$