Ciała i wielomiany

Javier de Lucas

Ćwiczenie 1. Załóż, że $(\mathbb{F}, +, \cdot, 1, 0)$ jest ciałem i $\alpha, \beta \in \mathbb{F}$. Które z następujących właściwości są prawdą?

1. $0 \cdot \alpha = 0$.
2. $(-1) \cdot \alpha = -\alpha$.
3. Każdy element zbioru $\mathbb{F}$ ma tylko jeden element przeciwny.
4. Każdy element $\alpha \neq 0$ zbioru $\mathbb{F}$ ma tylko jeden element odwrotny.
5. $(-\alpha) \cdot (-\beta) = \alpha \cdot \beta$.
6. $1 + 1 \neq 0$.
7. Jeżeli $\alpha \neq 0$ i $\beta \neq 0$, to $\alpha \cdot \beta \neq 0$.

Dowód:

1. Skoro $0 + 0 = 0$, to $0 \cdot \alpha = (0 + 0) \cdot \alpha$. Korzystając z rozdzielności mnożenia względem dodawania:
$$0 \cdot \alpha = 0 \cdot \alpha + 0 \cdot \alpha.$$
Wówczas,
$$0 \cdot \alpha + 0 \cdot \alpha + (-0 \cdot \alpha) = 0 \cdot \alpha + (-0 \cdot \alpha) = 0$$
i
$$0 \cdot \alpha = 0.$$
2. Wiemy, że $1 + (-1) = 0$. Więc, korzystając z poprzedniego wyniku
$$(1 + (-1)) \cdot \alpha = 0.$$
Z rozdzielności mnożenia względem dodawania i skoro $1 \cdot \alpha = \alpha$, wynika, że
$$1 \cdot \alpha + (-1) \cdot \alpha = \alpha + (-1) \cdot \alpha = 0 \ \Leftrightarrow \ (-1) \cdot \alpha = -\alpha.$$
Z tego, można wpisać $(-1) \cdot \alpha$ jako $-\alpha$. Aby uprościć notację, czesto się pisze $\alpha - \beta$ zamiast $\alpha + (-\beta)$.

3. Wprowadzamy dowód nie wprost (reductio ad absurdum). Niech α_1 i α_2 będą różnymi liczbami przeciwnymi do α. Z łączności dodawania, wynika, że

$$(\alpha_1 + \alpha) + \alpha_2 = \alpha_1 + (\alpha + \alpha_2).$$

Skoro $\alpha_1 + \alpha = \alpha + \alpha_2 = 0$, to

$$0 + \alpha_2 = \alpha_1 + 0 \Leftrightarrow \alpha_1 = \alpha_2$$

To sprzeczność. Więc, α tylko ma jeden element przeciwny.

4. Wprowadzamy dowód nie wprost. Niech α_1 i α_2 będą liczbami odwrotnymi do α. Z łączności mnożenia, wynika, że

$$(\alpha_1 \cdot \alpha) \cdot \alpha_2 = \alpha_1 \cdot (\alpha \cdot \alpha_2) \Rightarrow 1 \cdot \alpha_2 = \alpha_1 \cdot 1 \Leftrightarrow \alpha_1 = \alpha_2.$$

To sprzeczność. Więc, α ma tylko jeden element odwrotny.

5. Skoro istnieje tylko jeden element przeciwny do każdego elementu ciała, to

$$(-\alpha)(-\beta) = \alpha \cdot \beta \Leftrightarrow (-\alpha)(-\beta) - \alpha \cdot \beta = 0.$$

Teraz, udowodnimy prawą stronę. Z rozdzielności mnożenia względem dodawania i skoro $-\alpha \cdot \beta = (-1) \cdot \alpha \cdot \beta = (-\alpha) \cdot \beta$, wynika, że

$$(-\alpha) \cdot (-\beta) - \alpha \cdot \beta = (-\alpha) \cdot (-\beta) + (-\alpha) \cdot \beta = (-\alpha) \cdot (-\beta + \beta) = 0.$$

6. $1 + 1 \neq 0$ jest prawdą gdy charakterystyka ciała jest różna od 2. Na przykład, $\mathbb{Z}_2$ to ciało takie, że $1 + 1 = 0$, czyli $\mathbb{Z}_2$ ma charakterystykę 2.

7. Wprowadzamy dowód nie wprost. Zakładamy, że $\alpha, \beta \neq 0$ i $\alpha \cdot \beta = 0$ i to prowadzi do sprzeczności. Skoro $\alpha \neq 0$ i $\mathbb{F}$ jest ciałem, to α ma element odwrotny α^{-1} i

$$0 = \alpha \cdot \beta \Rightarrow 0 = \alpha^{-1} \cdot 0 = \alpha^{-1} \cdot \alpha \cdot \beta = \beta.$$

Więc, $\beta = 0$. To sprzeczność i $\alpha \cdot \beta \neq 0$.

□

Ćwiczenie 2. Udowodnij, że $(\mathbb{Z}_p, +, \cdot, 1, 0)$ jest ciałem wtedy i tylko wtedy p jest liczbą pierwszą.

Dowód: Wprowadźmy dowód nie wprost. Zakładamy, że $\mathbb{Z}_p$ jest ciałem i p nie jest liczbą pierwszą. Wówczas, można napisać $p = p_1 \cdot p_2$, gdzie $1 < p_2 < p$ i $p_1 > 1$ dla pewnych $p_1, p_2 \in \mathbb{N}$. Skoro $\mathbb{Z}_p$ jest ciałem i $p_1 \cdot p_2 = 0(\mathrm{mod\,p})$, to $p_1 = 0$ lub $p_2 = 0$ (mod p). To sprzeczność i $\mathbb{Z}_p$ nie jest ciałem.

Wiemy, że $\mathbb{Z}_p$ spełnia wszystkie właściwości ciała, oprócz ewentualnie istnienia elementu odwrotnego dla każdego $x \in \mathbb{Z}_p \backslash \{0\}$. Jeżeli p to liczba pierwsza, to możemy zdefiniować dla każdego $x \in \mathbb{Z}_p \backslash \{0\}$ jedną funkcję $\phi_x : y \in \mathbb{Z}_p \mapsto y \cdot x \in \mathbb{Z}_p$. To injekcja, ponieważ

$$\phi_x(y) = \phi_x(y') \Leftrightarrow y \cdot x = y' \cdot x \,(\mathrm{mod\ p}) \Leftrightarrow x(y - y') = 0 \ (\mathrm{mod\ p}).$$

Skoro x nie jest podzielny przez p, to $y = y'$ (mod p). Skoro dziedzina i przeciwdziedzina tego morfizmu mają taką samą skończoną liczbę elementów i ϕ_x jest injekcją, to ϕ_x jest surjekcją. Więc, istnieje y taki, że $x \cdot y = 1$ (mod p). To y jest elementem odwrotnym dla x. Wówczas, $\mathbb{Z}_p$ jest ciałem. □

Ćwiczenie 3. Udowodnij, że $\mathbb{R}[\mathfrak{X}]$ nie jest ciałem.

Dowód: Wystarczy podać przykład elementu w $\mathbb{R}[\mathfrak{X}]$ dla którego nie istnieje element odwrotny. Jeżeli istnieje element odwrotny, $P_0(\mathfrak{X})$, dla wielomianu $\mathfrak{X}$, mamy, że

$$\mathfrak{X} \cdot P_0(\mathfrak{X}) = 1.$$

To oznacza, że

$$0 = \deg(\mathfrak{X} P_0(\mathfrak{X})) = \deg(\mathfrak{X}) \deg(P_0(\mathfrak{X})) = \deg \mathfrak{X} + \deg(P_0(\mathfrak{X})) = 1 + \deg(P_0(\mathfrak{X})).$$

Nie istnieje wielomian stopnia -1. Wówczas, $\mathfrak{X}$ nie ma elementu odwrotnego i $\mathbb{R}[\mathfrak{X}]$ nie jest ciałem. □

Ćwiczenie 4. Niech $(\mathbb{F}, +, \cdot, 1, 0)$ będzie ciałem. Funkcją wymierną o współczynnikach w $\mathbb{F}$ nazywamy formalny napis postaci

$$f = \frac{f_1(\mathfrak{X})}{f_2(\mathfrak{X})},$$

gdzie $f_1(\mathfrak{X})$ i $f_2(\mathfrak{X})$ są wielomianami o współczynnikach w $\mathbb{F}$ i $f_2(\mathfrak{X}) \neq 0$. Ponadto, mówimy, że $f = g$, gdy $f_1(\mathfrak{X}) \cdot g_2(\mathfrak{X}) = g_1(\mathfrak{X}) \cdot f_2(\mathfrak{X})$. Zbiór funkcji wymiernych można wyposażyć w dodawanie i mnożenie

$$h + g = \frac{h_1(\mathfrak{X}) \cdot g_2(\mathfrak{X}) + h_2(\mathfrak{X}) g_1(\mathfrak{X})}{h_2(\mathfrak{X}) \cdot g_2(\mathfrak{X})}, \qquad h \cdot g = \frac{h_1(\mathfrak{X}) \cdot g_1(\mathfrak{X})}{h_2(\mathfrak{X}) \cdot g_2(\mathfrak{X})}.$$

Udowodnij, że zbiór funkcji wymiernych o współczynnikach w $\mathbb{F}$ jest ciałem względem tych działań.

Rozwiązanie: Działania $+$ i $\cdot$ są dobrze zdefiniowane, czyli dodawanie i mnożenie funkcji wymiernych są funkcjami wymiernymi. Zdefiniujemy 0 jako iloraz $0/1$ i 1 jako iloraz $1/1$.

- Widać, że $h + g = g + h$ i $hg = gh$ dla każdych funkcji wymiernych h, g.
- Mamy, że dla każdych funkcji wymiernych f, g, h:

$$\begin{aligned}
(f+g)+h &= \frac{f_1(\mathfrak{X}) \cdot g_2(\mathfrak{X}) + f_2(\mathfrak{X}) g_1(\mathfrak{X})}{f_2(\mathfrak{X}) \cdot g_2(\mathfrak{X})} + \frac{h_1(\mathfrak{X})}{h_2(\mathfrak{X})} \\
&= \frac{h_2(\mathfrak{X}) \cdot (f_1(\mathfrak{X}) \cdot g_2(\mathfrak{X}) + f_2(\mathfrak{X}) \cdot g_1(\mathfrak{X})) + h_1(\mathfrak{X}) \cdot f_2(\mathfrak{X}) \cdot g_2(\mathfrak{X})}{f_2(\mathfrak{X}) \cdot g_2(\mathfrak{X}) \cdot h_2(\mathfrak{X})} \\
&= \frac{f_2(\mathfrak{X}) \cdot (h_2(\mathfrak{X}) \cdot g_1(\mathfrak{X}) + g_1(\mathfrak{X}) \cdot h_2(\mathfrak{X})) + f_1(\mathfrak{X}) \cdot g_2(\mathfrak{X}) \cdot h_2(\mathfrak{X})}{f_2(\mathfrak{X}) \cdot g_2(\mathfrak{X}) \cdot h_2(\mathfrak{X})} \\
&= \frac{f_1(\mathfrak{X})}{f_2(\mathfrak{X})} + \frac{h_2(\mathfrak{X}) \cdot g_1(\mathfrak{X}) + g_1(\mathfrak{X}) \cdot h_2(\mathfrak{X})}{g_2(\mathfrak{X}) h_2(\mathfrak{X})} \\
&= \frac{f_1(\mathfrak{X})}{f_2(\mathfrak{X})} + \frac{g_1(\mathfrak{X})}{g_2(\mathfrak{X})} + \frac{h_1(\mathfrak{X})}{h_2(\mathfrak{X})} \\
&= f + (g + h)
\end{aligned}$$

i

$$\begin{aligned}
(f \cdot g) \cdot h &= \frac{f_1(\mathfrak{X}) \cdot g_1(\mathfrak{X})}{f_2(\mathfrak{X}) \cdot g_2(\mathfrak{X})} \cdot \frac{h_1(\mathfrak{X})}{h_2(\mathfrak{X})} = \frac{f_1(\mathfrak{X}) \cdot g_1(\mathfrak{X}) \cdot h_1(\mathfrak{X})}{f_2(\mathfrak{X}) \cdot g_2(\mathfrak{X}) \cdot h_2(\mathfrak{X})} \\
&= \frac{f_1(\mathfrak{X})}{f_2(\mathfrak{X})} \cdot \frac{g_1(\mathfrak{X}) \cdot h_1(\mathfrak{X})}{g_2(\mathfrak{X}) \cdot h_2(\mathfrak{X})} = f \cdot (g \cdot h).
\end{aligned}$$

- Widać, że $f+0=f$ i $f\cdot 1=f$ dla każdej funkcji wymiernej f.
- Jeżeli zdefiniujemy
$$-f\equiv\frac{-f_1(\mathfrak{X})}{f_2(\mathfrak{X})},\qquad f^{-1}\equiv\frac{f_2(\mathfrak{X})}{f_1(\mathfrak{X})}$$
widać, że $f+(-f)=f$ dla każdej funkcji wymiernej f i $f\cdot f^{-1}=1$ dla każdej funkcji wymiernej f różna od 0.
- Rozdzielność
$$\begin{aligned}(f+g)\cdot h&=\frac{f_1(\mathfrak{X})\cdot g_2(\mathfrak{X})+f_2(\mathfrak{X})g_1(\mathfrak{X})}{f_2(\mathfrak{X})\cdot g_2(\mathfrak{X})}\cdot\frac{h_1(\mathfrak{X})}{h_2(\mathfrak{X})}\\&=\frac{h_1(\mathfrak{X})\cdot(f_1(\mathfrak{X})\cdot g_2(\mathfrak{X})+f_2(\mathfrak{X})\cdot g_1(\mathfrak{X}))}{f_2(\mathfrak{X})\cdot g_2(\mathfrak{X})\cdot h_2(\mathfrak{X})}\\&=\frac{h_1(\mathfrak{X})\cdot f_1(\mathfrak{X})\cdot g_2(\mathfrak{X})+h_1(\mathfrak{X})\cdot f_2(\mathfrak{X})\cdot g_1(\mathfrak{X}))}{f_2(\mathfrak{X})\cdot g_2(\mathfrak{X})\cdot h_2(\mathfrak{X})}\\&=\frac{h_1(\mathfrak{X})\cdot f_1(\mathfrak{X})\cdot g_2(\mathfrak{X})}{f_2(\mathfrak{X})\cdot g_2(\mathfrak{X})\cdot h_2(\mathfrak{X})}+\frac{h_1(\mathfrak{X})\cdot f_2(\mathfrak{X})\cdot g_1(\mathfrak{X}))}{f_2(\mathfrak{X})\cdot g_2(\mathfrak{X})\cdot h_2(\mathfrak{X})}\\&=\frac{h_1(\mathfrak{X})\cdot f_1(\mathfrak{X})}{f_2(\mathfrak{X})\cdot h_2(\mathfrak{X})}+\frac{h_1(\mathfrak{X})\cdot g_1(\mathfrak{X})}{g_2(\mathfrak{X})\cdot h_2(\mathfrak{X})}\\&=f\cdot h+g\cdot h.\end{aligned}$$
dla dowolnych funkcji wymiernych f,g i h.

□

Ćwiczenie 5. Dane wielomiany

$$f_1(\mathfrak{X})=\mathfrak{X}^5+\mathfrak{X}^4+\mathfrak{X}^3+3\mathfrak{X}^2+\mathfrak{X}+1,\qquad f_2(\mathfrak{X})=\mathfrak{X}+1,\qquad f_3(\mathfrak{X})=\mathfrak{X}^2-1$$

w $\mathbb{R}[\mathfrak{X}]$, oblicz resztę podzielenia f_1 przez f_2 i f_3 za pomocą twierdzenia dzielenia wielomianów. Oblicz resztę gdy zakładamy, że $f_1,f_2,f_3\in\mathbb{Z}_5[\mathfrak{X}]$.

Dowód: Z twierdzenia o dzieleniu wielomianów wiemy, że istnieją wielomany $q(\mathfrak{X})$ i $r(\mathfrak{X})$ taki, że

$$f_1(\mathfrak{X})=q(\mathfrak{X})f_2(\mathfrak{X})+r(\mathfrak{X})$$

gdzie $\deg f_2>\deg r$. Skoro $\deg f_2=1$, to $r(\mathfrak{X})=c_0$, gdzie $c_0\in\mathbb{R}$. Dla $\xi=-1$, mamy, że $f_2(-1)=0$. Więc,

$$f_1(-1)=q(-1)f_2(-1)+c_0\Rightarrow f_1(-1)=c_0=2.$$

Z twierdzenia o dzieleniu wielomianów wiemy, że istnieją wielomiany $q(\mathfrak{X})$ i $r(\mathfrak{X})$ takie, że

$$f_1(\mathfrak{X}) = q(\mathfrak{X})f_3(\mathfrak{X}) + r(\mathfrak{X})$$

gdzie $\deg f_3 > \deg r$. Skoro $\deg f_3 = 2$, to $r(\mathfrak{X}) = c_1\mathfrak{X} + c_0$, gdzie $c_1, c_0 \in \mathbb{R}$. Dla $\xi = -1$, mamy, że $f_3(-1) = 0$. Więc,

$$f_1(-1) = q(-1)f_3(-1) + c_1(-1) + c_0 \Rightarrow f_1(-1) = -c_1 + c_0 = 2.$$

Dla $\xi = 1$, mamy, że $f_3(1) = 0$. Więc,

$$f_1(1) = q(1)f_3(1) + c_1 + c_0 \Rightarrow f_1(1) = c_1 + c_0 = 8.$$

Z tego wynika, że $c_1 = 3$ i $c_0 = 5$, czyli $r(\mathfrak{X}) = 3\mathfrak{X} + 5$.

Jeżeli zakładamy, że f_1, f_2, f_3 są wielomianami o współrzędnych w $\mathbb{Z}_5$, możemy powtarzać to samo jak wcześniej, tylko że liczby należą do $\mathbb{Z}_5$. Więc, ostatecznie mamy, że

1. Reszta podzielenia f_1 przez f_2 to 2
2. Reszta podzielenia f_1 przez f_3 to $3\mathfrak{X}$.

□