# Ciała

Javier de Lucas

Ciało można rozumieć jako uogólnienie zbioru liczb wymiernych $\mathbb{Q}$, liczb rzeczywistych $\mathbb{R}$ i liczb zespolonych $\mathbb{C}$.

*Ciało* to struktura $(\mathbb{K}, +, \cdot)$ taka, że:

- $+ : \mathbb{K} \times \mathbb{K}$ i $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ są funkcjami nazywanymi odpowiednio dodawaniem i mnożeniem,
- $(K, +, \cdot)$ to pierścień, tj:
  1. $(K, +)$ to grupa abelowa, tj.:
     - (łączność dodawania) $\forall_{a,b,c\in\mathbb{K}}\ a + (b + c) = (a + b) + c$,
     - (element neutralny dodawania) $\forall_{a\in\mathbb{K}}\ a + 0 = a$,
     - (element odwrotny dodawania) $\forall_{a\in\mathbb{K}}\ \exists_{b\in\mathbb{K}}\ a + b = 0$,
     - (przemienność dodawania) $\forall_{a,b\in\mathbb{K}}\ a + b = b + a$;
  2. (łączność mnożenia) $\forall_{a,b,c\in\mathbb{K}}\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
  3. (element neutralny mnożenia) $\forall_{a\in\mathbb{K}}\ a \cdot 1 = a$,
  4. (rozdzielność) $\forall_{a,b,c\in\mathbb{K}}\ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
  5. (przemienność mnożenia) $\forall_{a,b\in\mathbb{K}}\ a \cdot b = b \cdot a$.
- każdy niezerowy element $\mathbb{K}$ jest odwracalny, tzn:

$$\forall_{a\in\mathbb{K}\setminus\{0\}}\ \exists_{b\in\mathbb{K}}\ a \cdot b = 1,$$

Element 1 nazywa się *jedynką* lub *jednością* i jest on *elementem neutralnym mnożenia*.

Łatwo widać, że $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$, gdzie $+$ i $\cdot$ to zwykłe dodawanie i mnożenie, to są ciała.

Istnieją też ciała skończone, czyli $\mathbb{K}$ ma skończoną liczbę elementów. One są ważne w kryptografii i innych dziedzinach. Na przykład, niech $\mathbb{Z}_p$, gdzie $p$ to liczba pierwsza, będzie zbiórem $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. Zdefiniujemy nowe dodawanie $+_p$:

$$a +_p b \equiv (a + b) \bmod p.$$

Na przykład, dla $\mathbb{Z}_3$

$$0 +_p 0 = (0 + 0) \bmod 3 = 0, \qquad 2 +_p 1 = (2 + 1) \bmod 3 = 0,$$

$$1 +_p 1 = (1 + 1) \bmod 3 = 2, \qquad 2 +_p 2 = 4 \bmod 3 = 1.$$

Mnożenie zdefiniujemy podobnie

$$a \cdot_p b \equiv (a \cdot b) \bmod p.$$

Na przykład, dla $\mathbb{Z}_3$

$$0 \cdot_p 0 = (0 \cdot 0) \bmod 3 = 0, \qquad 2 \cdot_p 1 = (2 \cdot 1) \bmod 3 = 2,$$

$$1 \cdot_p 1 = (1 \cdot 1) \bmod 3 = 1, \qquad 2 \cdot_p 2 = 4 \bmod 3 = 1.$$

Można udowodnić, że $(\mathbb{Z}_p, +_p, \cdot_p)$ jest ciałem. Jedyna trudna część dowodu będzie udowodniona podczas ćwiczeń.

**Ćwiczenie 1.** Udowodnij, że jeżeli $p$ to liczba pierwsza, to $\sqrt{p} \notin \mathbb{Q}$, t.j. $\sqrt{p}$ nie jest liczbą wymierną.

**Ćwiczenie 2.** Pokaż, że $(\mathbb{Z}_p, +_p, \cdot_p)$ jest ciałem wtedy i tylko wtedy gdy $p$ to liczba pierwsza.

**Ćwiczenie 3.** Wykaż, że zbiór $\left\{p + \sqrt{2}q \,|\, p, q \in \mathbb{Q}\right\}$ wyposażony w standardowe mnożenie liczb jest ciałem.

**Ćwiczenie 4.** Wykaż, że

- $\sqrt[3]{9 + 4\sqrt{5}} \notin \mathbb{Q}$,
- $\sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}} = 3$,
- $\sqrt[3]{\sqrt{5} + 2} \notin \mathbb{Q}$,
- $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$,
- $\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} = 4$,
- $\sqrt[3]{2\sqrt{27} + 10} - \sqrt[3]{2\sqrt{27} - 10} = 2$.

**Ćwiczenie 5.** Zbadać, czy istnieją liczby wymierne $x, y \in \mathbb{Q}$, spełniające warunek

$$\sqrt[3]{2 + \sqrt{5}} = x + y\sqrt{5}.$$

**Ćwiczenie 6.** Wykaż, że nie istnieją liczby wymierne $a, b \in \mathbb{Q}$, takie, że

$$\sqrt[3]{4} = a + b\sqrt[3]{2}.$$