1 Ciało

Definicja 1. Zbiór K z działaniami dodawania $+$ oraz mnożenia $\cdot$ (których argumentami są dwa elementy z tego zbioru, a wartościami elementy z tego zbioru) nazywamy *ciałem*, jeśli zawiera co najmniej dwa elementy oraz spełnione są tzw. aksjomaty ciała:

- łączność dodawania: $\forall_{a,b,c\in K}(a+b)+c=a+(b+c)$,
- istnienie elementu neutralnego dodawania (zera): $\exists_{0\in K}\forall_{a\in K}a+0=a$,
- istnienie elementu przeciwnego: $\forall_{a\in K}\exists_{b\in K}a+b=0$,
- przemienność dodawania: $\forall_{a,b\in K}a+b=b+a$,
- łączność mnożenia: $\forall_{a,b,c\in K}(a\cdot b)\cdot c=a\cdot(b\cdot c)$,
- istnienie elementu neutralnego mnożenia (jedynki): $\exists_{1\in K}\forall_{a\in K}a\cdot 1=a$,
- przemienność mnożenia: $\forall_{a,b\in K}a\cdot b=b\cdot a$,
- rozdzielność mnożenia względem dodawania: $\forall_{a,b,c\in K}a\cdot(b+c)=a\cdot b+a\cdot c$,
- istnienie elementu odwrotnego (dla każdego niezerowego elementu): $\forall_{a\in K\setminus\{0\}}\exists_{b\in K}a\cdot b=1$.

Ciałami są na przykład: zbiór liczb rzeczywistych $\mathbb{R}$ (z dobrze znanymi działaniami), zbiór liczb wymiernych $\mathbb{Q}$, zbiór liczb zespolonych $\mathbb{C}$.

Ciało oprócz powyższych ma też inne często wykorzystywane własności, które wynikają wprost z aksjomatów. Poniżej podajemy przykłady takich własności. Formalne dowodzenie takich oczywistych faktów nie jest bynajmniej naszym celem, ale może być dobrym ćwiczeniem na zapoznanie się z definicją ciała – zwłaszcza, że będziemy korzystać nie tylko ze wspomnianych już ciał.

Twierdzenie 1. *Udowodnij, że w ciele występuje tylko jeden element neutralny dodawania (0), tylko jeden element neutralny mnożenia (1).*

Dowód. Załóżmy, że 0_1 oraz 0_2 są elementami neutralnymi dodawania. Wtedy $0_1=0_1+0_2=0_2$.

Zupełnie identycznie pokazuje się, że istnieje tylko jeden element neutralny mnożenia. □

Twierdzenie 2.

- $0\cdot a=0$ *dla dowolnego* $a\in K$.
- $0\neq 1$.
- *Dla dowolnego* $a\in K$ *element do niego przeciwny nie tylko istnieje, ale jest wyznaczony jednoznacznie; oznaczmy go* $-a$.
- *Dla dowolnego* $a\in K\setminus\{0\}$ *element do niego odwrotny nie tylko istnieje, ale jest wyznaczony jednoznacznie; oznaczmy go* a^{-1} *albo* $\frac{1}{a}$.

Dowód. Dowód pozostawiamy jako ćwiczenie. □

Definicja 2. $\mathbb{Z}_p$ oznacza zbiór $\{0, 1, \ldots, p-1\}$ z działaniami dodawania i mnożenia zdefiniowanymi tak, jak dla liczb całkowitych, ale modulo liczba pierwsza p.

Przykładowo, $\mathbb{Z}_5$ to zbiór $\{0, 1, 2, 3, 4\}$, w którym $1 + 2 = 3$, $2 + 4 = 6 \pmod 5 = 1$, $1 \cdot 4 = 4$, $3 \cdot 4 = 12 \pmod 5 = 2$.

Twierdzenie 3. *Dla dowolnej liczby pierwszej p zbiór $\mathbb{Z}_p$ z tak określonymi działaniami jest ciałem.*

Dowód. Większość własności ciała możecie sami sprawdzić. Nieoczywiste pozostaje tylko, czy dla każdego niezerowego elementu istnieje element odwrotny; jest to znane twierdzenie teorii liczb i nie będziemy go tutaj udowadniać. □

Bardzo ważnym ciałem jest $\mathbb{Z}_2$. Jest to zbiór $\{0, 1\}$ z działaniami takimi, że $0 + 0 = 0, 0 + 1 = 1 + 0 = 1, 1 + 1 = 0, 0 \cdot 0 = 0, 0 \cdot 1 = 1 \cdot 0 = 0, 1 \cdot 1 = 1$. Można na te działania patrzeć także jako na działania logiczne na wartościach logicznych: 0 – fałsz, 1 – prawda, $+$ – alternatywa rozłączna (tzw. *albo*), $\cdot$ – koniunkcja (tzw. *i*).

Definicja 3. *Charakterystyka* ciała K to najmniejsza niezerowa liczba jedynek tego ciała, jakie należy do siebie dodać, by otrzymać 0. Oznaczamy tę wartość jako $\mathrm{char}K$. Jeśli taka liczba nie istnieje, wtedy $\mathrm{char}K = 0$.

Przykładowo, charakterystyki $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ są równe 0. Z kolei $\mathrm{char}\mathbb{Z}_p = p$.

2 Liczby zespolone

O liczbach zespolonych możecie przeczytać na przykład na Wikipedii `http://pl.wikipedia.org/wiki/Liczby_zespolone` lub na stronie `http://www.ift.uni.wroc.pl/~cislo/algebra/wyklad5.pdf`. Z liczb zespolonych będziemy czasami korzystać, i chcielibyśmy, żebyście rozumieli: dodawanie, mnożenie, branie odwrotności, wzór de Moivre'a, sprzężenie, moduł i orientowali się, jak te definicje interpretować geometrycznie na płaszczyźnie.

3 Przestrzenie liniowe

3.1 Podstawy

Definicja 4. *Przestrzenią liniową* (lub *wektorową*) nad ciałem K nazywamy zbiór V z działaniami dodawania wektorów, które dowolnej parze elementów z V (*wektorów*) przyporządkowuje inny element z V (wektor), oraz mnożenia wektora przez skalar, które elementowi z ciała K (*skalarowi*) oraz elementowi z V (wektorowi) przyporządkowuje element z V (wektor); w V wyróżniony jest wektor *zerowy*, oznaczany jako 0, przy czym spełnione są następujące aksjomaty (dla dowolnych $u, v, w \in V$ oraz $a, b \in K$):

- łączność dodawania wektorów: $u + (v + w) = (u + v) + w$,
- przemienność dodawania wektorów: $u + v = v + u$,
- istnienie wektora neutralnego dodawania: $v + 0 = v$,
- rozdzielność mnożenia względem dodawania wektorów: $a \cdot (u + v) = a \cdot u + a \cdot v$,
- rozdzielność mnożenia względem dodawania skalarów: $(a + b) \cdot v = a \cdot v + b \cdot v$,
- łączność mnożenia przez skalary: $(a \cdot b) \cdot v = a \cdot (b \cdot v)$,
- 1 jest elementem neutralnym mnożenia: $v \cdot 1 = v$.

Nie należy się przerażać powyższymi aksjomatami. Wszystkie one obrazują proste własności, których żądamy od działań dodawania wektorów i ich mnożenia przez skalary.

Szczególną rolę pełnią przestrzenie K^n nad ciałem K. Przestrzeń K^n to zbiór ciągów n-elementowych o elementach z ciała K, czyli

$$K^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}$$

z naturalnie określonymi działaniami dodawania i mnożenia jako dodawanie i mnożenie po współrzędnych:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$
$$c \cdot (a_1, \ldots, a_n) = (c \cdot a_1, \ldots, c \cdot a_n).$$

Najbardziej znane są przestrzenie $\mathbb{R}^n$, w szczególności $\mathbb{R}^1 = \mathbb{R}$ czyli prosta rzeczywista, $\mathbb{R}^2$ czyli dobrze znana nam płaszczyzna, $\mathbb{R}^3$ czyli przestrzeń trójwymiarowa, którą postrzegamy dookoła siebie. Dodawanie wektorów w tych przestrzeniach zdefiniowaliśmy wygląda dokładnie tak, jak jest to pokazywane w szkole. Także mnożenie przez skalar, które jest po prostu jednokładnością o skali równej temu skalarowi, czyli odpowiednim rozciąganiem.

Znowu otrzymujemy kilka oczywistych własności:

Twierdzenie 4.
- *Dla każdego wektora v istnieje dokładnie jeden wektor przeciwny do niego u, czyli taki, że $v+u = 0$; oznaczamy go jako $-v$ i zachodzi równość $-v = (-1)\cdot v$.*
- $0v = 0$ *dla każdego wektora v oraz $a0 = 0$ dla dowolnego skalara a.*
- *Jeśli $av = 0$, to $a = 0$ lub $v = 0$.*

Dowód. Pozostawiamy dociekliwemu czytelnikowi. □

Definicja 5. Niepusty podzbiór $W \subset V$ przestrzeni liniowej V jest *podprzestrzenią liniową* przestrzeni liniowej V, jeśli jest zamknięty ze względu na działania dodawania oraz mnożenia przez skalar, czyli dla dowolnych $u, v \in W, a \in K$ zachodzi:

- $u + v \in W$,

- $av \in W$.

Łatwo sprawdzić, że działania dodawania i mnożenia w podprzestrzeni liniowej zachowują wszystkie swoje magiczne właściwości, wobec czego W z tymi działaniami spełnia aksjomaty przestrzeni liniowej – jest przestrzenią liniową.

Prostym przykładem może być podprzestrzeń $W = \{(a, a) : a \in \mathbb{R}\}$ przestrzeni $V = R^2$. V to cała płaszczyzna, W to prosta na płaszczyźnie opisana równaniem $y = x$.

3.2 Liniowa zależność, baza i wymiar przestrzeni

Definicja 6. *Kombinacją liniową* układu wektorów $v_1, \ldots, v_n$ o współczynnikach $a_1, \ldots, a_n$ nazywamy wektor

$$u = a_1 v_1 + \ldots a_n v_n = \sum_{i=1}^{n} a_i v_i.$$

Zauważmy, że jeśli u oraz w są pewnymi kombinacjami liniowymi wektorów $v_1, \ldots, v_n$, to $u + w$ oraz au dla dowolnego skalara a też są kombinacjami liniowymi tych wektorów.

Definicja 7. Przez $U = \text{lin}(v_1, \ldots, v_n)$ oznaczamy zbiór wszystkich kombinacji liniowych wektorów $v_1, \ldots, v_n$.

Jeśli wektory v_i należą do przestrzeni V, to U jest jej podprzestrzenią. Mówimy, że U jest *przestrzenią rozpiętą* na wektorach $v_1, \ldots, v_n$. Mówimy, że te wektory *rozpinają* przestrzeń V, jeśli $U = V$. W takiej sytuacji każdy wektor z V jest pewną kombinacją liniową wektorów z U.

Uwaga 1. Będziemy mówić, że układ współczynników $a_1, \ldots, a_n$ jest *niezerowy*, jeśli dla pewnego j zachodzi $a_j \neq 0$.

Może się zdarzyć, że kombinacja liniowa wektorów o niezerowym układzie współczynników będzie wektorem zerowym! Na przykład dla $a_1 = 1, a_2 = -1, v_1 = v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ mamy $a_1 v_1 + a_2 v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0.$

Definicja 8. Układ wektorów $v_1, \ldots, v_n$ nazywamy *liniowo zależnym*, jeśli dla pewnego niezerowego układu współczynników $a_1, \ldots, a_n$ ich kombinacja liniowa jest wektorem zerowym:

$$\sum_{i=1}^{n} a_i v_i = 0.$$

Jeśli nie istnieje taki niezerowy układ współczynników, to układ ten nazywamy *liniowo niezależnym*.

Równoważnie, układ $v_1, \ldots, v_n$ jest liniowo niezależny, wtedy i tylko wtedy, gdy równość $\sum_{i=1}^{n} a_i v_i = 0$ implikuje $a_1 = a_2 = \ldots a_n$. Jest to bardzo ważny fakt i czytelnik powinien się nad nim chwilę zastanowić.

Przykładowo, układ wektorów $\begin{pmatrix}1\\0\\0\end{pmatrix}$, $\begin{pmatrix}0\\1\\0\end{pmatrix}$, $\begin{pmatrix}0\\1\\1\end{pmatrix}$ jest liniowo niezależny (dlaczego?). Z kolei układ wektorów $\begin{pmatrix}0\\1\\1\end{pmatrix}$, $\begin{pmatrix}1\\-1\\1\end{pmatrix}$, $\begin{pmatrix}1\\0\\2\end{pmatrix}$ jest liniowo zależny (znajdź współczynniki!).

Jest jeszcze jeden ważny sposób patrzenia na liniową zależność wektorów.

Stwierdzenie 1. Układ $v_1, \ldots, v_n$ jest liniowo zależny wtedy i tylko wtedy, gdy jeden z tych wektorów da się otrzymać za pomocą pewnej kombinacji liniowej innych.

Dowód. Załóżmy, że układ ten jest liniowo zależny. Wtedy $\sum_{i=1}^{n} a_i v_i = 0$ dla niezerowego układu współczynników. Przyjmijmy bez utraty ogólności, że $a_1 \neq 0$. Wtedy

$$v_1 = \sum_{i=2}^{n} -\frac{a_i}{a_1} v_i,$$

co kończy dowód implikacji w jedną stronę. Dowód w drugą stronę pozostawiamy jako ćwiczenie. □

3.3 Przekształcenia liniowe

Definicja 9. Niech V, W będą przestrzeniami liniowymi nad ciałem K. Funkcję $\varphi : V \to W$ nazywamy *przekształceniem liniowym*, jeśli dla dowolnych $u, v \in V$ oraz dla każdego $a \in K$ zachodzi

- $\varphi(u + v) = \varphi(u) + \varphi(v)$,
- $\varphi(av) = a\varphi(v)$.

Definicja 10. *Jądrem* przekształcenia liniowego $\varphi : V \to W$ nazywamy zbiór

$$\ker \varphi = \{v \in V : \varphi(v) = 0\},$$

zaś *obrazem* nazywamy zbiór

$$\mathrm{im}\varphi = \{\varphi(v) : v \in V\}.$$

Definicja 11. Przekształcenie liniowe $\varphi : V \to W$ jest:

- *izomorfizmem*, jeśli jest bijekcją,
- *epimorfizmem*, jeśli jest na,
- *monomorfizmem*, jeśli jest różnowartościowe.

3.4 Iloczyn skalarny

$\mathbb{F}$ oznacza albo $\mathbb{R}$, albo $\mathbb{C}$ (można podstawić dowolne z nich).

Definicja 12. *Iloczynem skalarnym* $(\cdot,\cdot) : V \times V \to \mathbb{F}$ na przestrzeni V nad ciałem $\mathbb{F}$ nazywamy takie odwzorowania, które jest symetryczne, czyli $(u,v) = (v,u)$; dodatnio określone, czyli $(v,v) \in \mathbb{R}$ i $(v,v) > 0$ dla $v \neq 0$; dwuliniowe, czyli dla dowolnych $a, b \in \mathbb{F}, u, w, v \in V$ zachodzi $(au + bw, v) = a(u,v) + b(w,v)$ oraz $(v, au + bw) = a(v,u) + b(v,w)$.

Definicja 13. *Długością* wektora v nazywamy wartość $\|v\| = \sqrt{(v,v)}$.

Definicja 14. Iloczyn skalarny w przestrzeni $\mathbb{R}^n$ definiujemy nastepująco:

$$\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right) = x_1 y_1 + \ldots x_n y_n.$$

W przestrzeni $\mathbb{C}^n$ będzie to:

$$\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right) = x_1 \bar{y}_1 + \ldots x_n \bar{y}_n.$$

Można sprawdzić, że powyższe definicje w przestrzeniach $\mathbb{F}^n$ spełniają wcześniej podane aksjomaty. W szczególności definicja długości wektora i iloczynu skalarnego wektora w przestrzeniach $\mathbb{R}^2, \mathbb{R}^3$ jest taka sama, jaką znamy ze szkoły.