Algebra liniowa z geometrią

wykład I

Oznaczenia

$\mathbb{N}$ – zbiór liczb naturalnych, tutaj zaczynających się od 1

$\mathbb{Z}$ – zbiór liczb całkowitych

$\mathbb{Q}$ – zbiór liczb wymiernych

$\mathbb{R}$ – zbiór liczb rzeczywistych

$\mathbb{C}$ – zbiór liczb zespolonych

$\mathbb{H}$ – zbiór kwaternionów

Literatura

Lektura podstawowa

1. A. I. Kostrikin, *Wstęp do algebry*, części 1–3, PWN, Warszawa 2004–2005.

2. A. I. Kostrikin (red.), *Zbiór zadań z algebry*, PWN, Warszawa 2005.

Lektura uzupełniająca

1. A. Białynicki-Birula, *Algebra*, PWN, Warszawa 1971.

2. A. Białynicki-Birula, *Algebra liniowa z geometrią*, PWN, Warszawa 1976.

3. A. I. Kostrikin, J. I. Manin, *Algebra liniowa i geometria*, PWN, Warszawa 1993.

4. A. Mostowski, M. Stark, *Elementy algebry wyższej*, PWN, Warszawa 1972.

§1 Ciała liczbowe

Definicja 1 Podzbiór $\mathbb{F}$ zbioru liczb rzeczywistych nazywamy *ciałem liczbowym*, jeśli ma przynajmniej dwa elementy i dla każdej pary liczb a, b należących do $\mathbb{F}$ następujące liczby należą do $\mathbb{F}$: $a+b$, $a-b$, $a\cdot b$, a także $\frac{a}{b}$. W przypadku dzielenia zakładamy oczywiście, że $b\neq 0$.

Innymi słowy, ciało liczbowe to zbiór liczb liczący więcej niż jeden element, w którym wykonalne są wszystkie cztery działania.

Zbiór $\mathbb{N}$ nie jest ciałem liczbowym na przykład dlatego, że nie jest w nim wykonalne odejmowanie. W zbiorze $\mathbb{Z}$ nie jest wykonalne dzielenie, więc i $\mathbb{Z}$ nie jest ciałem liczbowym. Natomiast $\mathbb{Q}$ i $\mathbb{R}$ są ciałami.

Przykład 1 Niech $m>0$ będzie dowolną liczbą wymierną i niech $\mathbb{Q}[\sqrt{m}] := \{u+v\sqrt{m} : u,v\in\mathbb{Q}\}$. Ten ostatni zbiór jest ciałem. Dla przykładu pokażemy, że jest w nim wykonalne dzielenie.

Niech a i $b\in\mathbb{Q}[\sqrt{m}]$, przy tym niech $b\neq 0$. Wtedy istnieją liczby wymierne s, t, x, y, że $a=s+t\sqrt{m}$ i $b=x+y\sqrt{m}$. Jeśli b jest liczbą wymierną, to $u:=s/b$, $v:=t/b$ są wymierne oraz $a/b=u+v\sqrt{m}$. Jeśli zaś b nie jest liczba wymierną, to $c:=x-y\sqrt{m}$ jest także liczbą niewymierną, więc różną od 0. Mamy $\frac{a}{b}=\frac{ac}{bc}$. Zauważmy, że

$$ac=(sx-tym)+(tx-sy)\sqrt{m},\qquad bc=x^2-y^2m.$$

Pierwsza z liczb leży w $\mathbb{Q}[\sqrt{m}]$, druga jest wymierna. Ich iloraz, jak już wiemy na podstawie wcześniej rozpatrzonego przypadku, leży także w $\mathbb{Q}[\sqrt{m}]$, ale ten iloraz jest równy a/b.

Zauważmy, że ta sama argumentacja ma zastosowanie, jeśli zamiast $\mathbb{Q}$ wziąć jakiekolwiek ciało liczbowe $\mathbb{F}$, a w charakterze m wziąć dowolny element dodatni ciała $\mathbb{F}$. W konsekwencji, $\mathbb{F}[\sqrt{m}] := \{u+v\sqrt{m} : u,v\in\mathbb{F}\}$ jest ciałem.

Twierdzenie 1 *Jeżeli $\mathbb{F}$ jest ciałem liczbowym, to wszystkie liczby wymierne leżą w $\mathbb{F}$ ($\mathbb{Q}\subseteq\mathbb{F}$).*

Dowód. Ponieważ $|\mathbb{F}|\geqslant 2$, więc istnieje niezerowy element $a\in\mathbb{F}$. Dzielenie w $\mathbb{F}$ jest wykonalne, stąd $1=\frac{a}{a}\in\mathbb{F}$. Dalej, $\mathbb{N}\subseteq\mathbb{F}$, bo gdyby nie, to istniałaby taka najmniejsza liczba $n\in\mathbb{N}$, że $n\notin\mathbb{F}$. Jasne, że $n>1$. Zauważmy teraz, że $n=(n-1)+1$ oraz że oba składniki tej sumy są liczbami naturalnymi

mniejszymi niż n; muszą więc być elementami ciała $\mathbb{F}$. Ale w $\mathbb{F}$ wykonalne jest dodawanie, stąd $n \in \mathbb{F}$. I otrzymaliśmy sprzeczność.

Stąd że odejmowanie jest wykonalne w $\mathbb{F}$, mamy

$$0 = 1 - 1 \in \mathbb{F} \quad \text{i} \quad 0 - n = -n \in \mathbb{F},$$

o ile $n \in \mathbb{N}$. W konsekwencji $\mathbb{Z} \subseteq \mathbb{F}$. Ale jeżeli $w \in \mathbb{Q}$, to $w = \frac{p}{q}$, $p, q \in \mathbb{Z}$. Dzielenie jest w $\mathbb{F}$ wykonalne, więc $w \in \mathbb{F}$. □

Definicja 2 Powiemy, że a jest *liczbą algebraiczną stopnia* n, jeżeli istnieje wielomian stopnia n o współczynnikach wymiernych, $w(x) := a_0 + a_1 x + ... + a_n x^n$, że $w(a) = 0$ i nie ma wielomianu o współczynnikach wymiernych stopnia niższego, którego a byłaby pierwiastkiem.

Zadanie 1 Niech a – algebraiczna stopnia n. Udowodnić, że zbiór

$$\mathbb{Q}[a] := \{p_0 + p_1 a + p_2 a^2 + ... + p_{n-1} a^{n-1} : p_0, ..., p_{n-1} \in \mathbb{Q}\}$$

jest ciałem.

§2 Działania

Definicja 3 Załóżmy, że mamy zadany zbiór X. *Dwuargumentowym działaniem*, albo inaczej, *operacją* w X nazywamy przyporządkowanie każdej parze uporządkowanej zbioru X jednego elementu tego zbioru (różnym parom mogą być oczywiście przyporządkowane różne elementy).

Działania oznaczamy symbolami: $+$, $-$, $\cdot$, $\circ$, $\oplus$, $\otimes$ itp. Jeśli np. $\odot$ jest działaniem i $a, b \in X$, to element przyporządkowany parze uporządkowanej (a, b) oznaczamy $a \odot b$.

Przykład 2 Przyporządkowanie $\odot$ opisane wzorem $a \odot b = (a + b)^3$ jest działaniem w $\mathbb{R}$.

Definicja 4 Działanie $\odot$ w X jest *łączne*, jeśli dla każdych elementów $a, b, c \in X$

$$a \odot (b \odot c) = (a \odot b) \odot c.$$

Zauważmy, że dodawanie w $\mathbb{R}$ jest łączne, zaś odejmowanie nie.

DEFINICJA 5 Działanie $\odot$ w X jest *przemienne*, jeśli dla każdych $a, b \in X$

$$a \odot b = b \odot a.$$

Dodawanie w $\mathbb{R}$ jest oczywiście przemienne, zaś odejmowanie nie.

DEFINICJA 6 Jeśli w X są określone dwa działania $\oplus$, $\odot$, to $\odot$ jest *rozdzielne lewostronnie* względem $\oplus$, jeśli dla każdych $a, b, c \in X$

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c),$$

– *prawostronnie*, jeśli

$$(b \oplus c) \odot a = (b \odot a) \oplus (b \odot c).$$

ZADANIE 2 W $(0, +\infty)$ rozpatrzmy dwa działania: zwykłe dodawanie $+$ i *dodawanie harmoniczne*

$$a \oplus b = \frac{ab}{a+b}.$$

Czy $\oplus$ jest rozdzielne wzgędem $+$?

DEFINICJA 7 Element e nazywamy *elementem neutralnym* działania $\odot$ w X jeśli dla każdego elementu $x \in X$

$$e \odot x = x \odot e = x.$$

Oczywiście 0 jest elementem neutralnym dodawania liczb, zaś 1 – mnożenia. Dzielenie nie ma elementu neutralnego.

§3 Aksjomatyczna definicja ciała

DEFINICJA 8 Niech $\mathbb{F}$ będzie zbiorem z określonymi dwoma działaniami: dodawaniem $+$, i mnożeniem $\cdot$, w którym moŋa wyróżnić dwa niejednakowe elementy nazywane zwykle 0 i 1. $\mathbb{F}$ nazywamy *ciałem*, jeżeli dla dowolnych $x, y, z \in \mathbb{F}$:

(1) $x + y = y + x$,
(2) $x + (y + z) = (x + y) + z$,
(3) $x + 0 = x$,
(4) $\bigvee_t \quad x + t = 0$,

(5) $xy = yx$,
(6) $x \cdot (yz) = (xy) \cdot z$,
(7) $x \cdot 1 = x$,
(8) $x \neq 0 \Rightarrow \bigvee_u \quad xu = 1$,
(9) $x(y + z) = (xy) + (xz)$.

Wzory (1) – (9) nazywamy *aksjomatami ciała*.

Uwaga 1 Formuła (4) postuluje istnienie elementu *przeciwnego*, a (8) *odwrotnego*. Tak element przeciwny jak i odwrotny są *jedyne*.

Sprawdźmy na przykład jedyność elementu odwrotnego: Załóżmy, że u' i u są elementami odwrotnymi do x. Wtedy

$$u' = u' \cdot 1 = u' \cdot (xu) \overset{(6)}{=} (u'x) \cdot u \overset{(5)}{=} (xu') \cdot u = 1 \cdot u \overset{(5)}{=} u \cdot 1 \overset{(7)}{=} u.$$

Jedyny element przeciwny do x oznaczamy $-x$. Jedyny element odwrotny do x oznaczamy $\frac{1}{x}$, x^{-1}. Zamiast pisać $y+(-x)$ piszemy $y-x$ i tak określone działanie $-$ nazywamy *odejmowaniem*. Zamiast pisać $y \cdot \frac{1}{x}$ piszemy $\frac{y}{x}$, względnie y/x i tak określone działanie / nazywamy *dzieleniem*. Używamy więc tych samych terminów, co w arytmetyce.

§4 Przykłady ciał nieliczbowych.

1. Funkcja f argumentu rzeczywistego o wartościach rzeczywistych nosi nazwę *funkcji wymiernej*, jeżeli istnieje para wielomianów $p = a_0 + a_1x + ... + a_nx^n$, $q = b_0+b_1x+...+b_mx^m$, że $f(x) = \frac{p(x)}{q(x)}$, dla każdej takiej liczby x, że $q(x) \neq 0$. W takiej sytuacji piszemy $f = \frac{p}{q}$.

Niech $\mathbb{R}(x)$ oznacza zbiór wszystkich funkcji wymiernych. Wtedy zwykłe dodawanie i mnożenie funkcji są działaniami w $\mathbb{R}(x)$:

Jeżeli $f = \frac{p}{q}$, $g = \frac{r}{s} \in \mathbb{R}(x)$ i p, q, r, s – wielomiany, to

$$(1) \qquad f + g = \frac{\overbrace{ps + qr}^{\text{wielomian}}}{\underbrace{qs}_{\text{wielomian}}} \in \mathbb{R}(x),$$

$$(2) \qquad f \cdot g = \frac{\overbrace{pr}^{\text{wielomian}}}{\underbrace{qs}_{\text{wielomian}}} \in \mathbb{R}(x).$$

Łatwo zauważyć $\mathbb{R}(x)$ z działaniami $+, \cdot$ i elementami $0 =$ funkcja stała równa zero, $1 =$ funkcja stała równa jeden, spełnia aksjomaty (1) – (9); np. element odwrotny do $f = \frac{p}{q}$, to $f^{-1} = \frac{q}{p}$. Podobnie jak w $\mathbb{R}$, w $\mathbb{R}(x)$ można określić porządek. W tym celu, dla różnych elementów $f = \frac{p}{q}$, $g = \frac{r}{s}$ rozpatrzmy ich różnicę:

$$f - g = \frac{p}{q} - \frac{r}{s} = \frac{ps - qr}{qs}$$

Ponieważ licznik i mianownik są wielomianami, więc mają skończoną liczbę pierwiastków. W konsekwencji, począwszy od pewnej liczby u, dla wszystkich $x > u$ wielomiany te mają ciągle te same znaki. W konsekwencji, dla każdej liczby $x > u$,

$$(1) \qquad f(x) - g(x) > 0,$$

albo dla każdej liczby $x > u$,

$$(2) \qquad f(x) - g(x) < 0.$$

Przyjmijmy definicję porządku w $\mathbb{R}(x)$: $f < g$ jeżeli zachodzi (1), $g < f$ jeżeli zachodzi (2). Oczywiście, $f \leqslant g$ jeżeli zachodzi (1) lub $f = g$ oraz $g \leqslant f$ jeżeli zachodzi (2) lub $f = g$.

Zadanie 3 Udowodnić, że porządek określony w $\mathbb{R}(x)$ ma takie same własności, co zwykły porządek w $\mathbb{R}$, tzn. np.

- $f < g < h \Longrightarrow f < h$,
- $(f > 0, \quad g < h) \Longrightarrow fg < fh$.

Definicja 9 Powiemy, że podzbiór $\mathbb{G}$ ciała $\mathbb{F}$ jest *podciałem* ciała $\mathbb{F}$, jeżeli cztery podstawowe działania są w $\mathbb{G}$ wykonalne.

Alternatywnie, można tę definicję wyrazić tak: Spełnione są następujące warunki

- $0, 1 \in \mathbb{G}$,
- $x + y \in \mathbb{G}$ i $xy \in \mathbb{G}$, dla każdej pary x, $y \in \mathbb{G}$
- działania $+$, $\cdot$, w odniesieniu do elementów zbioru $\mathbb{G}$, spełniają aksjomaty (1) – (9).

2. Niech $\mathbb{F}$ – ciało liczbowe. Wtedy w taki sam sposób jak $\mathbb{R}(x)$ możemy określić $\mathbb{F}(x)$ (wielomiany p i q muszą mieć teraz współczynniki z $\mathbb{F}$). Pokazać, że $\mathbb{F}(x)$ jest podciałem ciała $\mathbb{R}(x)$.

3. Niech p – liczba pierwsza. Niech $\mathbb{Z}_p = \{0, 1, ..., p-1\}$. Określmy dodawanie $\oplus$ w $\mathbb{Z}_p$ wzorem

$$a \oplus b = \text{reszta z dzielenia } a + b \text{ przez } p,$$

zaś mnożenie –

$$a \odot b = \text{reszta z dzielenia } a \cdot b \text{ przez } p.$$

Oba działania są dobrze określone w $\mathbb{Z}_p$. Wyróżnijmy 0 i 1 w $\mathbb{Z}_p$.

TWIERDZENIE 2 *$\mathbb{Z}_p$ z wyróżnionymi elementami 0, 1 i działaniami $\oplus$, $\odot$ jest ciałem.*

Zanim przejdziemy do dowodu, przypomnimy kilka faktów i definicji.

ZADANIE 4 Dla dowolnych liczb x, y i $n \in \mathbb{N}$ zachodzi *wzór dwumianowy*, zwany też wzorem Newtona.

$$(\diamond) \qquad (x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + ... + \binom{n}{k}x^{n-k}y^k + ... + \binom{n}{n}x^0 y^n,$$

gdzie $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ jest liczbą naturalną równą liczbie podzbiorów k-elementowych w zbiorze n-elementowym, $n! = 1 \cdot 2 \cdot ... \cdot n$, $0! = 1$.

ZADANIE 5 Jeżeli p jest liczbą pierwszą, $k = 1, ..., p-1$, to p dzieli $\binom{p}{k}$.

DEFINICJA 10 Jeżeli dwie liczby całkowite x, y różnią się o krotność liczby $n \in \mathbb{N}$, to piszemy $x \equiv y \pmod{n}$ i czytamy x przystaje do y modulo n.

ZADANIE 6 Niech $x \equiv x' \pmod{n}$, $y \equiv y' \pmod{n}$. Wtedy

$(*)$ $\quad x + y \equiv x' + y' \pmod{n}$,

$(**)$ $\quad x \cdot y \equiv x' \cdot y' \pmod{n}$.

LEMAT 3 (MAŁE TWIERDZENIE FERMATA) *Dla każdej liczby całkowitej* x

$$x^p \equiv x \pmod{p}.$$

Dowód. Wystarczy założyć, że x jest liczbą naturalną. Gdyby x była niedodatnia, to dodalibyśmy na tyle dużą krotność lp liczby p, że $x + lp > 0$. Na mocy $(**)$

$$x^p \equiv (x + lp)^p \equiv x + lp \equiv x \pmod{p}.$$

$\uparrow$

pod warunkiem, że wiemy już, że twierdzenie jest prawdziwe dla liczb naturalnych

Jeżeli x jest teraz naturalna, to

$$\begin{aligned} x^p &= ((x-1)+1)^p \\ &\overset{(\diamond)}{=} (x-1)^p + \left(\binom{p}{1}(x-1)^{p-1} + ... + \binom{p}{p-1}(x-1)\right) + 1 \\ &\equiv (x-1)^p + 1 \pmod{p}, \end{aligned}$$

bo część objęta dużymi nawiasami jest krotnością p. Biorąc rozkład $x - 1 = (x-2) + 1$ i powtarzając rozumowanie, dostaniemy

$$(x-1)^p + 1 \equiv (x-2)^p + 2 \pmod{p}.$$

Z tych samych powodów

$$(x-2)^p + 2 \equiv (x-3)^p + 3 \pmod{p}$$

itd., aż dojdziemy do równości

$$1^p + (x-1) \equiv x \pmod{p}.$$

Porównując skrajne wyrażenia w wytworzonym ciągu równości, dostaniemy tezę. □

Wniosek 4 (małe twierdzenie Fermata – II postać) *Dla każdej liczby całkowitej x , niepodzielnej przez p*

$$x^{p-1} \equiv 1 \pmod{p}.$$

Dowód. Z lematu 3, $x^p - x = x(x^{p-1} - 1)$ dzieli się przez p. Ale p nie dzieli x, więc stąd, że p jest liczbą pierwszą wynika, iż p dzieli $x^{p-1} - 1$. □

Dowód tw. 2 Należy sprawdzić warunki (1) – (9). Warunki (1), (3), (5) i (7) są spełnione w sposób oczywisty. Fakt, że zachodzą warunki (2) i (6) sprawdza się w taki sam sposób, dlatego przeprowadzimy dowód (6). Z definicji $\odot$, dla każdej pary liczb $a, b \in \mathbb{Z}_p$ istnieje k - całkowita, że

$$a \cdot b = kp + (a \odot b).$$

Stąd mamy wzór

$$a \odot b \equiv a \cdot b \pmod{p}.$$

Stosując go w połączeniu ze wzorem $(**)$ z zadania 6 dostaniemy

$$\begin{aligned} x \odot (y \odot z) &\equiv x \cdot (y \odot z) \equiv x \cdot (y \cdot z) = (x \cdot y) \cdot z \\ &\equiv (x \odot y) \cdot z \equiv (x \odot y) \odot z \pmod{p}. \end{aligned}$$

Skrajne wyrazy leżą w $\mathbb{Z}_p$ i różnią się o krotność p, więc są równe.

W dowodzie (5) korzystamy z $(*)$. Dowód (9) jest też podobny: korzystamy zarówno z $(*)$, jak i z $(**)$. Co do (4), jeżeli $x \in \mathbb{Z}_p$, to szukanym elementem przeciwnym jest $p - x$, bo $x + (p - x) = p$, więc $x \oplus (p - x) = 0$.

I wreszcie dowód (8).

Niech $x^{\odot k} = \underbrace{x \odot ... \odot x}_{k-\text{krotnie}}$. Z dowiedzionej już łączności wynika że wyrażenie po prawej stronie ma sens. Zastosujmy wniosek 4. Wtedy

$$x \odot x^{\odot(p-2)} = x^{\odot(p-1)} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Ponieważ $x \odot x^{\odot(p-2)}$ i 1 różnią się o krotność p i leżą w $\mathbb{Z}_p$, więc

$$x \odot x^{\odot(p-2)} = 1.$$

W rezultacie $x^{\odot(p-2)}$ jest szukanym elementem odwrotnym u. □

§5 Izomorfizm ciał

Niech p – liczba pierwsza. Niech k oznacza jakąkolwiek liczbę całkowitą i niech $X = \{k, k+1, ..., k+p-1\}$. Określmy dodawanie $\oplus_k$ w X i mnożenie $\odot_k$ w X wzorami:

$$x \oplus_k y = [(x - k) \oplus (y - k)] + k, \qquad x \odot_k y = [(x - k) \odot (y - k)] + k.$$

Można sprawdzić, że X jest ciałem p-elementowym, tak jak $\mathbb{Z}_p$, z elementami neutralnymi: k – dodawania, $k + 1$ – mnożenia. Elementy $\mathbb{Z}_p$ i X możemy ustawić we wzajemnej odpowiedniości:

$$\begin{array}{cccccc} 0 & 1 & 2 & ... & p-1 \\ k & k+1 & k+2 & ... & k+(p-1) \end{array}$$

Zauważmy, że jeżeli elementy a, b należą do X i a', b' są odpowiadającymi im elementami w $\mathbb{Z}_p$ (tzn. $a' = a - k$, $b' = b - k$), to $a \oplus b$ i $a' \oplus_k b'$ także odpowiadają sobie. Podobnie $a \odot b$ i $a' \odot_k b'$. Możemy powiedzieć, że ciała $\mathbb{Z}_p$ i X są algebraicznie identyczne. Mówiąc nieformalnie, są jedynie *zrobione z innego materiału*.

Definicja 11 Dano dwa ciała $\mathbb{F}$ i $\mathbb{G}$. Powiemy, że ciała te są *izomorficzne*, jeśli istnieje odwzorowanie $\varphi : \mathbb{F} \to \mathbb{G}$ o następujących własnościach:

(1) φ jest różnowartościowe i *na*,

(2) $\bigwedge\limits_{x,y\in\mathbb{F}} \varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{i} \quad \varphi(xy) = \varphi(x) \cdot \varphi(y).$

Odwzorowanie φ nazywamy *izomorfizmem* ciał $\mathbb{F}$ i $\mathbb{G}$.

Zadanie 7 Jeśli φ jest izomorfizmem ciał to $\varphi(0) = 0$ i $\varphi(1) = 1$.

Rozwiązanie. Z (2) wynika, że

$$\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0).$$

Odejmując $\varphi(0)$ od obu stron dostajemy $0 = \varphi(0)$. Ponieważ odwzorowanie φ jest różnowartościowe, więc $\varphi(1) \neq 0$. Znowu z (2)

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1).$$

Dzieląc obie strony przez $\varphi(1)$ dostajemy $1 = \varphi(1)$. □

Definicja 12 *Automorfizmem* ciała $\mathbb{F}$ nazywamy każdy izomorfizm $\varphi : \mathbb{F} \to \mathbb{F}$.

§6 Charakterystyka ciała

Niech $\mathbb{F}$ będzie ciałem oraz niech 1 będzie jedynką tego ciała, zaś 0 jego zerem. Możliwa jest jedna z dwu sytuacji:

(1) $\bigwedge\limits_{n\in\mathbb{N}} \quad n1 = \underbrace{1+...+1}_{n-\text{krotnie}} \neq 0,$

(2) $\bigvee\limits_{n\in\mathbb{N}} \quad n1 = 0.$

Jeżeli zachodzi pierwsza sytuacja, to mówimy, że ciało ma *charakterystykę* 0 i piszemy $\chi(\mathbb{F}) = 0$. W drugim przypadku, bierzemy m – najmniejszą spośród n, dla których $n1 = 0$ i mówimy, że $\mathbb{F}$ ma charakterystykę m, i piszemy $\chi(\mathbb{F}) = m$.

TWIERDZENIE 5 *Jeżeli $\chi(\mathbb{F}) \neq 0$, to $\chi(\mathbb{F})$ jest liczbą pierwszą.*

LEMAT 6 *Jeżeli $\mathbb{F}$ – ciało, $x, y \in \mathbb{F}$ i $x \neq 0 \neq y$, to $x \cdot y \neq 0$.*

Dowód. Niech x^{-1}, y^{-1} – elementy odwrotne do x, y. Gdyby $x \cdot y = 0$, to wtedy

$$(y^{-1}x^{-1}) \cdot (xy) = (y^{-1}x^{-1})0 = 0, \quad \text{(dlaczego?)}$$

a z drugiej strony,

$$\begin{aligned}(y^{-1}x^{-1}) \cdot (xy) &= y^{-1} \cdot (x^{-1} \cdot (xy)) = y^{-1} \cdot ((x^{-1}x)y) \\ &= y^{-1}(1 \cdot y) = y^{-1} \cdot y = 1.\end{aligned}$$

Otrzymaliśmy sprzeczność. □

Dowód tw. 5. Gdyby $m = \chi(\mathbb{F})$ nie była liczbą pierwszą, to $m = k \cdot l$, gdzie $k, l \in \mathbb{N}$ i $k, l \neq 1$. Stąd

$$0 = m1 = (k1) \cdot (l1).$$

Na mocy lematu 6, $k1 = 0$ lub $l1 = 0$, co przeczyłoby definicji m (jako charakterystki ciała $\mathbb{F}$) bo tak k jak i l byłyby mniejsze niż m. □

TWIERDZENIE 7 *Jeżeli $\mathbb{F}$ i $\mathbb{G}$ – dwa ciała, $\varphi : \mathbb{F} \to \mathbb{G}$ spełnia warunki:*

(1) $\varphi(x + y) = \varphi(x) + \varphi(y)$,

(2) $\varphi(x \cdot y) = \varphi(x)\varphi(y)$,

(3) $\bigvee_{u \in \mathbb{F}} \varphi(u) \neq 0$,

to zbiór $\varphi(\mathbb{F}) = \{\varphi(x) : x \in \mathbb{F}\}$ jest ciałem oraz φ jest izomorfizmem ciał $\mathbb{F}$ i $\varphi(\mathbb{F})$.

Dowód. Niech u – element zapewniony przez (3). Na mocy (2) mamy

$$\varphi(u) = \varphi(u \cdot 1) = \varphi(u)\varphi(1),$$

skoro $\varphi(u) \neq 0$, to istnieje $\varphi(u)^{-1}$. Mnożąc ostatnie równanie stronami przez $\varphi(u)^{-1}$ dostaniemy

$$1 = \varphi(u^{-1})\varphi(u) = \underbrace{(\varphi(u)^{-1}\varphi(u))}_{1}\varphi(1) = \varphi(1).$$

1 leży więc w $\varphi(\mathbb{F})$; podobnie jak w zadaniu 7 dowodzimy, że $0 = \varphi(0)$, stąd 0 leży w $\varphi(\mathbb{F})$. Warunki (1) i (2) oznaczają, że w $\varphi(\mathbb{F})$ wykonalne jest dodawanie

i mnożenie. By przekonać się, że $\varphi(\mathbb{F})$ jest ciałem, pozostaje sprawdzić, że elementy tego zbioru spełniają (4) i (8) aksjomat ciała.

Istnienie elementu odwrotnego:

Niech $y \in \varphi(\mathbb{F})$ i $y \neq 0$. Wtedy istnieje $x \neq 0$, że $\varphi(x) = y$. Mamy

$$y \cdot \varphi(x^{-1}) = \varphi(x) \cdot \varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1.$$

Stąd $y^{-1} = \varphi(x^{-1}) \in \varphi(\mathbb{F})$.

Podobnie dowodzi sie istnienia elementu przeciwnego. Żeby ostatecznie stwierdzić, że φ jest izomorfizmem, musimy pokazać, że φ jest różnowartościowe, tzn. że dla każdej pary $x, x' \in \mathbb{F}$ zachodzi

$$x \neq x' \Rightarrow \varphi(x) \neq \varphi(x').$$

Gdyby $\varphi(x) = \varphi(x')$, to dodając do obu stron $\varphi(-x')$ dostalibyśmy

$$\varphi(x - x') = \varphi(x' - x') = \varphi(0) = 0.$$

Ale $x - x' \neq 0$, zatem mnożąc przez $\varphi((x - x')^{-1})$ dostalibyśmy

$$1 = \varphi(1) = \varphi((x - x') \cdot (x - x')^{-1}) = \varphi(x - x') \cdot \varphi((x - x')^{-1}) = 0.$$

Co nie jest możliwe. □

TWIERDZENIE 8 *(1) Jeżeli $\chi(\mathbb{F}) = 0$, to ciało $\mathbb{F}$ zawiera podciało izomorficzne z $\mathbb{Q}$.*

(2) Jeżeli $\chi(\mathbb{F}) = p \neq 0$, to ciało $\mathbb{F}$ zawiera podciało izomorficzne z $\mathbb{Z}_p$.

Dowód.

Ad.(1) Rozpatrzmy zbiór $\mathbb{G} \subseteq \mathbb{F}$ składający się z wszystkich elementów postaci $\frac{k\cdot 1}{m\cdot 1}$, gdzie $k \in \mathbb{Z}$, $m \in \mathbb{N}$. Zbiór $\mathbb{G}$ jest ciałem, bo jest zamknięty na cztery podstawowe operacje. Określmy $\varphi : \mathbb{Q} \to \mathbb{F}$ wzorem

$$\varphi\left(\frac{k}{m}\right) = \frac{k \cdot 1}{m \cdot 1}.$$

Łatwo zauważyć, że φ jet poprawnie określonym odwzorowaniem, niezależnym od sposobu przedstawienia liczb wymiernych, tzn.

$$\frac{k}{m} = \frac{k'}{m'} \Rightarrow \varphi\left(\frac{k}{m}\right) = \varphi\left(\frac{k'}{m'}\right).$$

Oczywiście $\varphi(\mathbb{Q}) = \mathbb{G}$. Pokażemy, korzystając z twierdzenia 7, że $\mathbb{G}$ jest ciałem izomorficznym z $\mathbb{Q}$. Ponieważ (3) jest spełnione, bo

$$\bigwedge_{u\in\mathbb{Q}\setminus\{0\}} \varphi(u) \neq 0,$$

wystarczy sprawdzić, że spełnione są warunki (1) i (2), zróbmy to np. dla warunku (1):

$$\varphi\left(\frac{k}{m} + \frac{r}{s}\right) = \varphi\left(\frac{ks + rm}{ms}\right) = \frac{(ks + rm)\cdot 1}{(ms)\cdot 1} = \frac{k\cdot 1}{m\cdot 1} + \frac{r\cdot 1}{s\cdot 1} = \varphi\left(\frac{k}{m}\right) + \varphi\left(\frac{r}{s}\right).$$

Ad.(2) Definiujemy odwzorowanie $\varphi : \mathbb{Z}_p \to \mathbb{F}$ wzorem $\varphi(k) = k\cdot 1$, $k \in \mathbb{Z}_p$, i sprawdzamy (ćwiczenie!), że φ spełnia założenia twierdzenia 7. W rezultacie $\mathbb{G} = \varphi(\mathbb{Z}_p) = \{0, 1\cdot 1, ..., (p-1)\cdot 1\}$ okazuje się być ciałem izomorficznym z $\mathbb{Z}_p$. □

§7 Liczby zespolone