ROZDZIAŁ XIII

# CIAŁA LICZBOWE

**§ 1. Definicja ciała liczbowego. Przykłady.** *Ciałem liczbowym* nazywamy każdy niepusty zbiór liczb zespolonych, w którym wykonalne są cztery działania arytmetyczne z wyjątkiem dzielenia przez zero.

Innymi słowy: na to, żeby zbiór liczb zespolonych $Z$ był ciałem liczbowym, potrzeba i wystarcza, aby posiadał następujące własności:

I. Jeżeli $z_1$ i $z_2$ są liczbami należącymi do zbioru $Z$, to $z_1+z_2$, $z_1-z_2$ i $z_1z_2$ również są liczbami należącymi do zbioru $Z$;

II. Jeżeli nadto $z_2\neq 0$, to $z_1:z_2$ też jest liczbą należącą do zbioru $Z$.

Zbiór $\mathcal{R}$ wszystkich liczb wymiernych jest ciałem liczbowym, podobnie jak zbiór $\mathcal{E}$ wszystkich liczb rzeczywistych, jako też zbiór $\mathcal{C}$ wszystkich liczb zespolonych. Zbiór złożony z jednej tylko liczby 0 też jest ciałem liczbowym, ponieważ warunki I i II są dla niego prawdziwe. Zbiór wszystkich liczb zespolonych postaci $a+bi$, gdzie $a$ i $b$ są liczbami wymiernymi, też jest oczywiście ciałem liczbowym.

Jako inny przykład ciała liczbowego, weźmy zbiór $\mathcal{Z}$ wszystkich liczb rzeczywistych postaci $a+b\sqrt{2}$, gdzie $a$ i $b$ są liczbami wymiernymi. Łatwo stwierdzamy, że jeżeli liczby $z_1$ i $z_2$ należą do zbioru $\mathcal{Z}$, to liczby $z_1+z_2$, $z_1-z_2$ i $z_1z_2$ też należą do $\mathcal{Z}$; wynika to ze wzorów:

$$(a_1+b_1\sqrt{2})\pm(a_2+b_2\sqrt{2}) = (a_1\pm b_1)+(a_2\pm b_2)\sqrt{2},$$
$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = a_1a_2+2b_1b_2+(a_1b_2+a_2b_1)\sqrt{2}.$$

Aby wreszcie okazać, że jeżeli $z_1$ i $z_2$ należą do $\mathcal{Z}$ oraz $z_2\neq 0$, to $z_1:z_2$ też należy do $\mathcal{Z}$, wystarczy zauważyć, że jeżeli $a_2+b_2\sqrt{2}\neq 0$, to:

$$\frac{a_1+b_1\sqrt{2}}{a_2+b_2\sqrt{2}} = \frac{(a_1+b_1\sqrt{2})(a_2-b_2\sqrt{2})}{a_2^2-2b_2^2} = \frac{a_1a_2-2b_1b_2}{a_2^2-2b_2^2}+\frac{a_2b_1-a_1b_2}{a_2^2-2b_2^2}\sqrt{2},$$

przy czym $a_2^2-2b_2^2\neq 0$, gdyż liczby $a_2$ i $b_2$ są wymierne i nie są obie równe zeru, ponieważ $a_2+b_2\sqrt{2}\neq 0$, zaś liczba $\sqrt{2}$ nie jest wymierną. Zbiór $\mathcal{Z}$ jest więc ciałem liczbowym.



Ciało $\mathcal{Z}$ ma następującą własność: *nie istnieje żadne ciało liczbowe zawarte między $\mathcal{R}$ a $\mathcal{Z}$*, t.j. żadne ciało różne od $\mathcal{R}$ i od $\mathcal{Z}$, zawarte w $\mathcal{Z}$ i zawierające $\mathcal{R}$.

Istotnie, jeżeli $Z_1$ jest ciałem zawartym w $\mathcal{Z}$ i zawierającym $\mathcal{R}$, ale różnym od $\mathcal{R}$, to $Z_1$ zawiera conajmniej jedną liczbę niewymierną $z_1$ należącą do $\mathcal{Z}$, a więc liczbę postaci $z_1=a_1+b_1\sqrt{2}$, gdzie $a_1$ i $b_1$ są to liczby wymierne oraz $b_1\neq 0$. Skoro jednak $z_1$ należy do ciała liczbowego $Z_1$, to i liczba $\sqrt{2}=\frac{z_1-a_1}{b_1}$ należy do $Z_1$, a więc też i każda liczba postaci $a+b\sqrt{2}$, gdzie $a$ i $b$ są liczbami wymiernymi, czyli każda liczba ciała $\mathcal{Z}$. Zatem $\mathcal{Z}\subset Z_1$ [1]), a że z założenia jest $Z_1\subset\mathcal{Z}$, więc $Z_1=\mathcal{Z}$, co dowodzi zapowiedzianej własności ciała $\mathcal{Z}$.

Podobną własność posiada też ciało liczbowe utworzone ze wszystkich liczb postaci $a+b\sqrt{D}$, gdzie $a$ i $b$ są to liczby wymierne (dowolne), zaś $D$ jest liczbą wymierną (stałą dla danego ciała), nie będącą kwadratem liczby wymiernej.

Zbiór wszystkich liczb algebraicznych jest w myśl wniosku z twierdzenia 3 Rozdziału XII (§ 3, str. 215) ciałem liczbowym, podobnie jak zbiór wszystkich liczb algebraicznych rzeczywistych.

*Każde ciało liczbowe zawiera liczbę* 0. Jeżeli bowiem $Z$ jest ciałem liczbowym, a $z$ jakąkolwiek liczbą należącą do $Z$, to liczba $z-z=0$ należy do $Z$.

*Jeżeli ciało liczbowe zawiera choć jedną liczbę różną od zera, to zawiera każdą liczbę wymierną.* Jeżeli bowiem liczba $z_0\neq 0$ należy do ciała liczbowego $Z$, to $z_0:z_0=1$ należy do $Z$. Jeżeli zaś liczba $n$ należy do $Z$, to i liczba $n+1$ należy do $Z$, skąd drogą indukcji wnosimy, że każda liczba naturalna $n$ należy do $Z$. Z uwagi na to, że 0 należy do $Z$ i że $-n=0-n$, wnosimy stąd dalej, że każda liczba całkowita należy do $Z$, a więc i każdy iloraz liczby całkowitej przez liczbę naturalną, czyli każda liczba wymierna.

Udowodniliśmy w ten sposób

***Twierdzenie 1.*** *Ciało $\mathcal{R}$ liczb wymiernych jest częścią każdego ciała liczbowego, nie redukującego się do jednej tylko liczby* 0.

Twierdzenie to wyrażamy krótko, mówiąc, że $\mathcal{R}$ jest *najmniejszym* ciałem liczbowym (nie redukującym się do liczby 0).

ĆWICZENIA. 1. Dowieść, że zbiór wszystkich liczb rzeczywistych postaci $a+b\sqrt[3]{2}$, gdzie liczby $a$ i $b$ są wymierne, nie jest ciałem liczbowym.

Dowód. Gdyby zbiór ten był ciałem liczbowym, mielibyśmy $(\sqrt[3]{2})^2=a+b\sqrt[3]{2}$, gdzie liczby $a$ i $b$ są wymierne; wówczas $\sqrt[3]{2}$ byłoby liczbą algebraiczną stopnia $\leqslant 2$, wbrew temu, co wiemy z Rozdziału XII, § 2 (str. 213).

2. Dowieść, że zbiór wszystkich liczb rzeczywistych postaci $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, gdzie liczby $a$, $b$ i $c$ są wymierne, jest ciałem liczbowym.

[1]) Znak $\subset$ (używany w Teorii mnogości) znaczy „zawiera się w".

**§ 2. Rozszerzanie ciał liczbowych przez dołączanie nowych liczb.** Udowodnimy następujące

***Twierdzenie 2.*** *Jeżeli $Q$ jest dowolnym zbiorem liczb zespolonych (niekoniecznie ciałem liczbowym), to istnieje najmniejsze ciało liczbowe $K$ zawierające $Q$*, t. j. takie ciało liczbowe $K$ zawierające $Q$, które jest zawarte w każdym ciele liczbowym, zawierającym $Q$.

Dowód. Istnieją oczywiście ciała liczbowe, zawierające zbiór $Q$, np. ciało wszystkich liczb zespolonych. Zaliczmy do zbioru $K$ każdą taką i tylko taką liczbę $z$, która należy do każdego ciała liczbowego $Z$ zawierającego $Q$. Zbiór $K$ będzie oczywiście zawierał zbiór $Q$ i będzie zawarty w każdym ciele liczbowym zawierającym $Q$. Wystarczy więc jeszcze tylko okazać, że zbiór $K$ jest ciałem liczbowym.

Załóżmy w tym celu, że liczby $z_1$ i $z_2$ należą do $K$. Jeżeli $Z$ jest dowolnym ciałem liczbowym, zawierającym $Q$, to w myśl określenia zbioru $K$ liczby $z_1$ i $z_2$ należą do $Z$, a więc (z uwagi na to, że $Z$ jest ciałem liczbowym) liczby $z_1+z_2$, $z_1-z_2$, $z_1z_2$ oraz w przypadku, gdy $z_2\neq 0$, również liczba $z_1:z_2$, należą do $Z$. Liczby te należą więc do każdego ciała liczbowego $Z$ zawierającego $Q$, a zatem, w myśl określenia zbioru $K$, muszą być zaliczone do $K$. Zbiór $K$ jest więc ciałem liczbowym, c. b. d. o.

W szczególności, jeżeli $Q$ jest ciałem liczbowym, a $\alpha$ liczbą nie należącą do $Q$, to istnieje najmniejsze ciało liczbowe, zawierające ciało $Q$ i liczbę $\alpha$.

Ciało takie będziemy oznaczali przez $Q(\alpha)$ i mówili, że powstało przez *dołączenie* (adjunkcję) liczby $\alpha$ do ciała $Q$.

Udowodnimy o nim następujące

***Twierdzenie 3.*** *Ciało $Q(\alpha)$ jest zbiorem $Z$ wszystkich liczb postaci $\frac{\varphi(\alpha)}{\psi(\alpha)}$, gdzie $\varphi$ i $\psi$ są wielomianami o współczynnikach należących do $Q$, przy czym $\psi(\alpha)\neq 0$.*

Dowód. Z założenia, że $Q$ jest ciałem liczbowym, wynika łatwo, że zbiór $Z$ jest ciałem liczbowym. Otóż każda liczba zbioru $Z$ należy do $Q(\alpha)$. Ale i na odwrót, zbiór $Q(\alpha)$ jest zawarty w $Z$, gdyż $Z$ jest ciałem liczbowym, zawierającym zbiór $Q$ i liczbę $\alpha$; zaś $Q(\alpha)$ jest według określenia częścią każdego takiego ciała liczbowego. Wynika stąd, że $Z=Q(\alpha)$, c. b. d. o.



PRZYKŁADY. Jeżeli $Q$ jest zbiorem wszystkich liczb rzeczywistych, to $Q(i)$ jest zbiorem wszystkich liczb zespolonych.

Jeżeli $Q$ jest zbiorem wszystkich liczb wymiernych, to $Z=Q(\sqrt{2})$ jest zbadanym w § 1 zbiorem $\mathcal{Z}$ wszystkich liczb rzeczywistych postaci $a+b\sqrt{2}$, gdzie liczby $a$ i $b$ są wymierne.

Łatwo dowieść, że *część wspólna dwóch* (a nawet dowolnej skończonej lub nieskończonej mnogości) *ciał liczbowych jest ciałem liczbowym.*

Ale połączenie dwóch ciał liczbowych w jeden zbiór może już nie być ciałem liczbowym. Np. zbiór $\mathcal{R}(\sqrt{2})+\mathcal{R}(\sqrt{3})$ nie jest ciałem liczbowym, gdyż zawiera liczby $\sqrt{2}$ i $\sqrt{3}$, lecz nie zawiera liczby $\sqrt{2}+\sqrt{3}$, ponieważ — jak można dowieść — ani $\mathcal{R}(\sqrt{2})$, ani $\mathcal{R}(\sqrt{3})$ tej liczby nie zawiera.

Natomiast *suma ciągu nieskończonego ciał liczbowych, z których każde jest zawarte w następnym, jest ciałem liczbowym.*

W szczególności np. ciałem liczbowym jest zbiór:

$$K=K(\sqrt{2})+K(\sqrt[4]{2})+K(\sqrt[8]{2})+\ldots+K(\sqrt[2^n]{2})+\ldots$$

Ciało $K$ zawiera ciąg nieskończony rosnący różnych podciał:

$$K(\sqrt{2}),\quad K(\sqrt[4]{2}),\quad K(\sqrt[8]{2}),\quad \ldots$$

Istnieją też ciała, zawierające ciąg nieskończony malejący różnych podciał. Własność tę ma np. ciało $K(\alpha)$, gdzie $\alpha$ jest dowolną liczbą przestępną (np. $\alpha=\pi$); zawiera ono ciąg malejący różnych podciał:

$$K(\alpha^2),\ K(\alpha^4),\ \ldots,\ K(\alpha^{2^n}),\ \ldots$$

**§ 3. Wielomiany nieprzywiedlne w ciele liczbowym.** Wielomian (stopnia $n>0$) o współczynnikach należących do ciała liczbowego $K$ nazywamy *przywiedlnym* w tym ciele, jeżeli jest iloczynem dwóch wielomianów niższego stopnia o współczynnikach należących do $K$.

W przeciwnym razie nazywamy go *nieprzywiedlnym* w ciele $K$.

Np. wielomian $x^2+1$ jest nieprzywiedlny w ciele $\mathcal{R}$ wszystkich liczb wymiernych, ale jest przywiedlny w ciele $\mathcal{R}(i)$. W ciele wszystkich liczb zespolonych każdy wielomian stopnia większego od 1 jest przywiedlny, gdyż na mocy twierdzenia 20 Rozdziału VIII (§ 11, str. 125) rozkłada się na iloczyn czynników liniowych.

W ciele $\mathcal{C}$ wszystkich liczb rzeczywistych przywiedlnym jest każdy wielomian o współczynnikach rzeczywistych stopnia $n>2$ (Rozdział VIII, § 11, wniosek 2 z twierdzenia 21, str. 128).

***Twierdzenie 4.*** *Jeżeli $f(x)$ jest wielomianem o współczynnikach należących do ciała liczbowego $K$, a $a$ jest pierwiastkiem tego wielomianu, to wielomian $f(x)$ jest przywiedlny w ciele $K(a)$.*

Dowód. Wielomian $f(x)$ jest wówczas podzielny przez $x-a$, a iloraz z tego dzielenia jest w myśl twierdzenia 2 Rozdziału VIII (§ 1, str. 104) wielomianem, którego współczynniki otrzymują się za pomocą działań wymiernych ze współczynników wielomianów $f(x)$ i $x-a$, a zatem należą do ciała liczbowego $K(a)$.

Z twierdzenia 6 Rozdziału VIII (§ 4, str. 110) wynika następujące

***Twierdzenie 5.*** *Jeżeli współczynniki dwu wielomianów $f(x)$ i $g(x)$ należą do ciała liczbowego $K$, to i współczynniki ich największego wspólnego dzielnika należą do $K$.*

Na podstawie twierdzenia 5 udowodnimy

***Twierdzenie 6.*** *Jeżeli $f(x)$ i $g(x)$ są wielomianami o współczynnikach należących do ciała liczbowego $K$ i jeżeli wielomian $g(x)$ jest nieprzywiedlny w ciele $K$, to albo wielomiany $f(x)$ i $g(x)$ są względnie pierwsze, albo wielomian $f(x)$ jest podzielny przez $g(x)$.*

Dowód. Niech $d(x)$ oznacza największy wspólny dzielnik wielomianów $f(x)$ i $g(x)$. Na mocy twierdzenia 5 współczynniki wielomianu $d(x)$ należą do ciała liczbowego $K$, jak również współczynniki ilorazu $g(x):d(x)$.

Ponieważ wielomian $g(x)$ jest nieprzywiedlny w ciele $K$, więc iloraz $g(x):d(x)$ nie może być wielomianem stopnia dodatniego, niższego od stopnia wielomianu $g(x)$. Jeżeli $d(x)$ jest stopnia 0 (czyli $d(x)=1$), to wielomiany $f(x)$ i $g(x)$ są względnie pierwsze; jeżeli zaś $d(x)$ jest tego samego stopnia co $g(x)$, to iloraz $g(x):d(x)$ jest liczbą stałą, skąd wynika, że wielomian $f(x)$ jest podzielny przez $g(x)$, c. b. d. o.

***Wniosek.*** *Jeżeli $f(x)$ i $g(x)$ są wielomianami o współczynnikach należących do ciała liczbowego $K$, przy czym wielomian $g(x)$ jest nieprzywiedlny w ciele $K$, i jeżeli dla pewnego pierwiastka $\alpha_1$ wielomianu $g(x)$ mamy $f(\alpha_1)=0$, to $f(\alpha)=0$ dla każdego pierwiastka $\alpha$ wielomianu $g(x)$.*

Jeżeli bowiem $f(\alpha_1)=0$ i $g(\alpha_1)=0$, to wielomiany $f$ i $g$ mają wspólny pierwiastek, a więc nie mogą być względnie pierwsze. W myśl twierdzenia 6 wielomian $f(x)$ jest więc podzielny przez $g(x)$, a przeto znika dla każdego pierwiastka wielomianu $g(x)$.



***Twierdzenie 7.*** *Jeżeli $p$ jest liczbą pierwszą, zaś $a$ liczbą zespoloną należącą do ciała liczbowego $K$, lecz nie będącą $p$-tą potęgą żadnej liczby ciała $K$, to dwumian $x^p-a$ jest nieprzywiedlny w ciele $K$.*

Dowód. Przypuśćmy, że

$$x^p-a=\varphi(x)\psi(x), \tag{1}$$

gdzie $\varphi(x)$ i $\psi(x)$ są wielomianami stopnia niższego niż $p$ o współczynnikach należących do ciała $K$. Możemy więc założyć, że

$$\varphi(x)=x^m+b_1x^{m-1}+\ldots+b_m, \tag{2}$$

gdzie $m<p$, a liczby $b_1, \ldots, b_m$ należą do ciała $K$. Niech $r$ oznacza którykolwiek z pierwiastków $p$-go stopnia z liczby $a$ (np. główny). Jest więc $r^p=a$ i — jak wiemy z twierdzenia 8 Rozdziału VI (§ 8, str. 97) — wszystkimi pierwiastkami wielomianu $x^p-a$ są liczby:

$$r,\ \varepsilon r,\ \varepsilon^2 r,\ \ldots,\ \varepsilon^{p-1}r, \tag{3}$$

gdzie $\varepsilon$ jest pierwiastkiem pierwotnym $p$-go stopnia z jedności (np. $\varepsilon=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$).

Wobec (1) każdy z pierwiastków wielomianu (2) jest jedną z liczb (3). Iloczyn wszystkich pierwiastków wielomianu (2) wynosi więc $\varepsilon^k r^m$, gdzie $k$ jest pewną liczbą całkowitą. Ponieważ zaś, jak wiemy z Rozdziału VIII (§ 11, wzory (41), str. 126), liczba $b=(-1)^m b_m$ jest iloczynem wszystkich pierwiastków wielomianu (2), więc $b=\varepsilon^k r^m$, skąd wobec $r^p=a$ i $\varepsilon^p=1$ znajdujemy:

$$b^p=(\varepsilon^k r^m)^p=(\varepsilon^p)^k\cdot a^m=a^m. \tag{4}$$

Z założenia, że $p$ jest liczbą pierwszą i że $m<p$, wynika, że liczby $m$ i $p$ są względnie pierwsze. Istnieją więc liczby całkowite $t$ i $u$ takie, iż $pt+mu=1$, skąd wobec (4):

$$a=a^{pt+mu}=(a^t b^u)^p.$$

Zatem $a$ byłoby $p$-tą potęgą liczby $a^t b^u$, należącej do ciała $K$, wbrew założeniu.

***Twierdzenie 8.*** *Jeżeli $g(x)$ jest wielomianem stopnia $m$ o współczynnikach należących do ciała liczbowego $K$, nieprzywiedlnym w tym ciele, zaś $\alpha$ jest pierwiastkiem wielomianu $g(x)$, to każda liczba ciała liczbowego $K(\alpha)$ daje się, i to w jeden tylko sposób, przedstawić w postaci:*

$$\xi=c_0+c_1\alpha+c_2\alpha^2+\ldots+c_{m-1}\alpha^{m-1}, \tag{5}$$

*gdzie $c_0, c_1, \ldots, c_{m-1}$ są liczbami należącymi do $K$.*

Dowód. Niech $\xi$ oznacza liczbę ciała $K(\alpha)$. W myśl twierdzenia 3 liczba $\xi$ daje się więc przedstawić w postaci:

$$\xi = \frac{\varphi(\alpha)}{\psi(\alpha)}, \tag{6}$$

gdzie $\varphi$ i $\psi$ są wielomianami o współczynnikach należących do $K$, przy czym $\psi(\alpha) \neq 0$.

Otóż wielomiany $\psi(x)$ i $g(x)$ są względnie pierwsze. W przeciwnym bowiem razie wielomiany te posiadałyby wspólny pierwiastek $\beta$. Wobec jednak nieprzywiedlności wielomianu $g(x)$ wielomian $\psi(x)$ byłby w myśl twierdzenia 6 podzielny przez $g(x)$, a wobec $g(\alpha)=0$ byłoby też $\psi(\alpha)=0$, wbrew założeniu.

Wielomiany $\psi(\alpha)$ i $g(x)$ są więc względnie pierwsze. Na mocy twierdzenia 7 z Rozdziału VIII (§ 5, str. 112) istnieją zatem wielomiany $f(x)$ i $h(x)$ takie, iż tożsamościowo:

$$f(x)\psi(x) + h(x)g(x) = 1, \tag{7}$$

przy czym — jak wiemy z twierdzenia 6 Rozdziału VIII (§ 4, str. 110) — współczynniki tych wielomianów powstają ze współczynników wielomianów $\psi$ i $g$ za pomocą działań wymiernych, co dowodzi, że współczynniki wielomianów $f(x)$ i $h(x)$ należą do ciała liczbowego $K$.

Podstawiając w (7) $x=\alpha$, otrzymamy z uwagi na to, że $g(\alpha)=0$ i $\psi(\alpha)\neq 0$;

$$\frac{1}{\psi(\alpha)} = f(\alpha),$$

zatem wobec (6):

$$\xi = \varphi(\alpha) f(\alpha). \tag{8}$$

Z twierdzeń 1 i 2 Rozdziału VIII (§ 1, str. 103 i 104) wynika dalej, że istnieją takie wielomiany $k(x)$ i $l(x)$ o współczynnikach należących do ciała liczbowego $K$, iż tożsamościowo:

$$\varphi(x)f(x) = k(x)g(x) + l(x), \tag{9}$$

przy czym stopień wielomianu $l(x)$ jest niższy niż stopień wielomianu $g(x)$. Wielomian $l(x)$ ma więc postać:

$$l(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1}x^{m-1}, \tag{10}$$

gdzie $c_0, c_1, \ldots, c_{m-1}$ są liczbami należącymi do ciała $K$. Wobec $g(\alpha)=0$ wzory (8), (9) i (10) dają wzór (5).



Aby zakończyć dowód, wystarczy więc jeszcze okazać, że jeżeli:

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{m-1}\alpha^{m-1} = c_0' + c_1'\alpha + c_2'\alpha^2 + \ldots + c_{m-1}'\alpha^{m-1}, \tag{11}$$

gdzie $c_0, c_1, \ldots, c_{m-1}, c_0', c_1', \ldots, c_{m-1}'$ są liczbami należącymi do ciała $K$, to:

$$c_i = c_i' \quad \text{dla} \quad i = 0,1,\ldots,m-1. \tag{12}$$

Załóżmy więc, że zachodzi równość (11) i przyjmijmy:

$$W(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1}x^{m-1} - (c_0' + c_1'x + c_2'x^2 + c_{m-1}'x^{m-1}).$$

$W(x)$ jest więc wielomianem stopnia niższego niż $m$ o współczynnikach należących do $K$. Wobec (11) jest $W(\alpha)=0$, ponieważ zaś $g(\alpha)=0$, a wielomian $g(x)$ jest nieprzywiedlny w ciele $K$, więc wielomian $W(x)$ jest w myśl twierdzenia 9 podzielny przez $g(x)$. Z uwagi, że $\operatorname{st} g(x) = m > \operatorname{st} W(x)$, jest to możliwe tylko wtedy, gdy wielomian $W(x)$ jest tożsamościowo równy 0 i gdy zachodzą wzory (11).

Twierdzenie 8 zostało więc udowodnione w zupełności.

Wynika z niego natychmiast następujący

***Wniosek.*** *Jeżeli $\alpha$ jest liczbą algebraiczną stopnia $m$, to każda liczba ciała $\mathcal{R}(\alpha)$ daje się, i to w jeden tylko sposób, przedstawić w postaci* (5), *gdzie $c_0, c_1, \ldots, c_{m-1}$ są liczbami wymiernymi.*

***Twierdzenie 9.*** *Jeżeli $f(x)$ i $g(x)$ są wielomianami w ciele liczbowym $K$, których stopnie $p$ i $q$ są liczbami pierwszymi, a których współczynniki należą do ciała $K$; jeżeli dalej $g(\alpha)=0$ i wielomian $f(x)$ staje się przywiedlnym w ciele $K(\alpha)$, to $p=q$.*

Dowód. Niechaj w ciele $K(\alpha)$ istnieje dla wielomianu $f(x)$ rozkład:

$$f(x) = \varphi(x)\psi(x), \tag{13}$$

przy czym współczynniki wielomianów $\varphi$ i $\psi$ należą do $K(\alpha)$; zatem, w myśl twierdzenia 8, są one postaci (5) dla $m=q$, gdzie $c_0, c_1, \ldots, c_{q-1}$ są liczbami ciała $K$. Możemy więc przyjąć:

$$\varphi(x) = \varphi(x,\alpha), \qquad \psi(x) = \psi(x,\alpha), \tag{14}$$

gdzie $\varphi(x,\alpha)$ i $\psi(x,\alpha)$ są wielomianami względem $x$ i $\alpha$ o współczynnikach należących do $K$, przy czym stopnie $m$ i $n$ tych wielomianów względem $x$ są mniejsze od $p$.

Wobec (13) i (14) mamy tożsamościowo względem $x$:

$$f(x) = \varphi(x,\alpha)\psi(x,\alpha). \tag{15}$$

Możemy oczywiście napisać:

$$\varphi(x,\alpha)\psi(x,\alpha)=A_0(\alpha)+A_1(\alpha)x+A_2(\alpha)x^2+\ldots+A_p(\alpha)x^p, \tag{16}$$

gdzie $A_0, A_1, \ldots, A_p$ są wielomianami względem $\alpha$ o współczynnikach należących do $K$.

Jeżeli teraz

$$f(x)=a_0+a_1x+\ldots+a_px^p, \tag{17}$$

to wobec tożsamości (15) i (16), mamy:

$$A_0(\alpha)-a_0=0, \quad A_1(\alpha)-a_1=0 \quad \ldots, \quad A_p(\alpha)-a_p=0.$$

Wielomiany $A_i(x)-a_i$ dla $i=0,1,\ldots,p$ mają współczynniki należące do $K$ i znikają dla pierwiastka $\alpha$ wielomianu $g(x)$, nieprzywiedlnego w ciele $K$.

W myśl wniosku z twierdzenia 1 wielomiany te znikają więc dla każdego pierwiastka wielomianu $g(x)$. Niech

$$\alpha=\alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

będą wszystkimi pierwiastkami wielomianu $g(x)$. Zatem:

$$A_i(\alpha_j)-a_i=0 \quad \text{dla} \quad i=0,1,\ldots,p-1 \quad \text{i} \quad j=1,2,\ldots,q,$$

skąd wobec (15), (16) i (17):

$$f(x)=\varphi(x,\alpha_j)\psi(x,\alpha_j) \quad \text{dla } j=1,2,\ldots,q,$$

a więc

$$[f(x)]^q=\prod_{j=1}^{q}\varphi(x,\alpha_j)\prod_{j=1}^{q}\psi(x,\alpha_j). \tag{18}$$

Uporządkujmy wielomiany:

$$\Phi(x)=\prod_{j=1}^{q}\varphi(x,\alpha_j) \quad \text{i} \quad \Psi(x)=\prod_{j=1}^{q}\psi(x,\alpha_j) \tag{19}$$

według potęg zmiennej $x$. Współczynniki tych wielomianów będą oczywiście wielomianami względem $\alpha_1,\alpha_2,\ldots,\alpha_q$ o współczynnikach należących do $K$, przy czym będą to wielomiany symetryczne względem $\alpha_1,\alpha_2,\ldots,\alpha_q$. W myśl twierdzenia 2 Rozdziału IX (§ 3, str. 159) dadzą się więc one wyrazić wymiernie przez współczynniki równania $g(x)=0$ i liczby ciała $K$, a więc będą należały do $K$. Wobec (18) i (19) mamy zatem tożsamość:

$$[f(x)]^q=\Phi(x)\Psi(x), \tag{20}$$

gdzie wobec (19) wielomian $\Phi(x)$ jest stopnia $qm$, zaś wielomian $\Psi(x)$ — stopnia $qn$.



Wobec nieprzywiedlności wielomianu $f(x)$ w ciele $K$ oraz z uwagi na to, że współczynniki wielomianów $f(x)$, $\Phi(x)$ i $\Psi(x)$ należą do $K$, ze wzoru (20) wynika z łatwością, że wielomiany $\Phi(x)$ i $\Psi(x)$ są potęgami wielomianu $f(x)$, pomnożonymi przez liczby stałe.

Przypuśćmy, że (abstrahując od stałej) $\Phi(x)$ jest $\mu$-tą, zaś $\Psi(x)$ $\nu$-tą potęgą wielomianu $f(x)$. Będzie więc wobec $\operatorname{st} f(x)=p$:

$$p\mu=qm \quad \text{i} \quad p\nu=qn. \tag{21}$$

Ponieważ $m<p$, więc liczba (naturalna) $m$ jest pierwsza względem liczby pierwszej $p$ i wzór (21) dowodzi, że liczba $q$ musi być podzielna przez $p$; ponieważ zaś liczby $p$ i $q$ są pierwsze, więc $p=q$, c. b. d. o.

## § 4. Kolejne dołączanie liczb algebraicznych do ciała liczb wymiernych.

Mamy następujące

***Twierdzenie 10.*** *Jeżeli $\alpha$ i $\beta$ są dowolnymi liczbami algebraicznymi i jeżeli $K_1=\mathcal{R}(\alpha)$, zaś $K_2=K_1(\beta)$, to istnieje taka liczba algebraiczna $\gamma$, że $K_2=\mathcal{R}(\gamma)$.*

Innymi słowy:

*Kolejne dołączanie dwu (a więc i dowolnej skończonej ilości) liczb algebraicznych do ciała liczb wymiernych jest równoważne dołączeniu do tego ciała tylko jednej odpowiednio dobranej liczby algebraicznej.*

Dowód. Niech liczby algebraiczne $\alpha$ i $\beta$ będą odpowiednio pierwiastkami wielomianów nieprzywiedlnych $f(x)$ i $g(x)$ o współczynnikach wymiernych. Nie wykluczamy przy tym przypadku, w którym $f(x)=g(x)$. Niech dalej $\alpha_1=\alpha, \alpha_2, \ldots, \alpha_m$ będą wszystkimi pierwiastkami wielomianu $f(x)$, a $\beta_1=\beta, \beta_2, \ldots, \beta_n$ — wszystkimi pierwiastkami wielomianów $g(x)$. Istnieje oczywiście liczba naturalna $k$, różna od każdej z liczb:

$$\frac{\alpha_i-\alpha_j}{\beta_r-\beta_s},$$

gdzie $i$ i $j$ są dwiema różnymi liczbami ciągu $1,2,\ldots,m$, zaś $r$ i $s$ — dwiema różnymi liczbami ciągu $1,2,\ldots,n$.

Okażemy, że

$$K_2=\mathcal{R}(\alpha-k\beta). \tag{22}$$

Przyjmijmy:

$$\gamma_{p,q}=\alpha_p+k\beta_q \quad \text{dla } p=1,2,\ldots,m \quad \text{i} \quad q=1,2,\ldots,n. \tag{23}$$

Jeżeli $p$ i $p'$ są dwiema różnymi liczbami ciągu $1,2,\ldots,m$, zaś $q$ i $q'$ dwiema różnymi liczbami ciągu $1,2,\ldots,n$, to — jak wynika z określenia liczby $k$ — zachodzi nierówność:

$$k \neq \frac{\alpha_p - \alpha_{p'}}{\beta_q - \beta_{q'}},$$

z której wynika, że

$$\gamma_{p,q} - \gamma_{p',q'} = \alpha_p - \alpha_{p'} + k(\beta_q - \beta_{q'}) \neq 0.$$

Liczby $\gamma_{p,q}$, gdzie $p=1,2,\ldots,m$ i $q=1,2,\ldots,n$, są więc wszystkie różne, przy czym $\gamma_{1,1} = \alpha_1 - k\beta_1 = \alpha - k\beta$.

Przyjmijmy:

$$F(x) = \prod_{p=1}^{m} \prod_{q=1}^{n} (x - \gamma_{p,q}). \tag{24}$$

Współczynniki wielomianu $F(x)$ są wobec (23) funkcjami symetrycznymi zarówno liczb $\alpha_1,\alpha_2,\ldots,\alpha_m$, jak liczb $\beta_1,\beta_2,\ldots,\beta_n$. W myśl twierdzenia o funkcjach symetrycznych (Rozdział IX, § 3, tw. 2, str. 159) i wobec wymierności współczynników wielomianów $f(x)$ i $g(x)$, są więc one liczbami wymiernymi.

Niech $p$ będzie jedną z liczb $1,2,\ldots,m$, zaś $q$ jedną z liczb $1,2,\ldots,n$. Wobec (24) i (23) funkcja wymierna $F_{p,q}(x)$, określona wzorem

$$F_{p,q}(x) = \frac{F(x)}{x - \gamma_{p,q}} \tag{25}$$

jest na mocy twierdzenia 2 Rozdziału VIII (§ 1, str. 104) wielomianem względem $x$, którego współczynniki są wielomianami względem $\alpha_p$ i $\beta_q$ (o współczynnikach wymiernych).

Niech teraz $\theta$ będzie daną liczbą ciała $K_2 = K_1(\beta)$, gdzie $K_1 = \mathcal{R}(\alpha)$. Z twierdzenia 8 wynika, że liczba $\theta$ daje się przedstawić jako wielomian względem $\alpha$ i $\beta$ o współczynnikach wymiernych. Oznaczmy go przez $W(\alpha,\beta)$ i przyjmijmy:

$$\Phi(x) = \sum_{p=1}^{m} \sum_{q=1}^{n} W(\alpha_p,\beta_q) F_{p,q}(x);$$

jest to oczywiście wielomian względem $x$, którego współczynniki są funkcjami symetrycznymi zarówno względem $\alpha_1,\alpha_2,\ldots,\alpha_m$, jak względem $\beta_1,\beta_2,\ldots,\beta_n$, a zatem liczbami wymiernymi.



Dla $\gamma = \gamma_{1,1}$ zachodzi równość:

$$\Phi(\gamma) = W(\alpha,\beta) F_{1,1}(\gamma),$$

gdyż $F_{p,q}(\gamma) = \dfrac{F(\gamma)}{\gamma - \gamma_{p,q}} = 0$ dla $p>1$ i $q>1$. Zatem:

$$\theta = W(\alpha,\beta) = \frac{\Phi(\gamma)}{F_{1,1}(\gamma)}. \tag{26}$$

Lecz wobec (24) i (25) oraz wobec $\gamma = \gamma_{1,1}$ mamy zgodnie z określeniem pochodnej wielomianu (Rozdział VIII, § 2, str. 105):

$$F_{1,1}(\gamma) = F'(\gamma),$$

gdzie $F'$ jest pochodną wielomianu $F$. Wzór (26) dowodzi zatem, że liczba $\theta$ należy do ciała $\mathcal{R}(\gamma)$. Tym sposobem dowiedliśmy, że ciało $K_2$ jest częścią ciała $\mathcal{R}(\gamma)$.

Z drugiej strony, jeżeli $\alpha$ należy do ciała $K_1 = \mathcal{R}(\alpha)$, to należy tym bardziej do ciała $K_2 = K_1(\beta)$; ponieważ zaś $\beta$ należy do $K_1(\beta)$, więc i liczba $\gamma = \gamma_{1,1} = \alpha - k\beta$ należy do ciała $K_2$. Wnosimy stąd, że ciało $\mathcal{R}(\gamma)$ jest częścią ciała $K_2$.

Ciała $K_2$ i $\mathcal{R}(\gamma)$ są więc identyczne, c. b. d. o.

Badanie ciał liczbowych, otrzymywanych przez kolejne dołączanie liczb algebraicznych (skończenie wiele razy) do ciała liczb wymiernych, sprowadza się zatem do badania ciał $\mathcal{R}(\alpha)$, gdzie $\alpha$ jest liczbą algebraiczną.

## § 5. Przedstawianie pierwiastków równania $z^n - 1 = 0$ za pomocą pierwiastników stopnia mniejszego od $n$.

O liczbie zespolonej $z$ mówimy, że *daje się przedstawić za pomocą pierwiastników*, jeżeli istnieje ciąg skończony liczb zespolonych $\alpha_1,\alpha_2,\ldots,\alpha_m$ oraz ciąg skończony liczb naturalnych $q_1,q_2,\ldots,q_m$ takich, że jeżeli przyjmiemy $R_0 = \mathcal{R}$ (gdzie $\mathcal{R}$ jest ciałem liczb wymiernych) oraz $R_k = R_{k-1}(\alpha_k)$ dla $k=1,2,\ldots,m$, to $\alpha_k^{q_k}$ należy do $R_{k-1}$ dla $k=1,2,\ldots,m$, zaś $z$ należy do $R_m$.

Możemy założyć, że liczby $q_1,q_2,\ldots,q_n$ są pierwsze. Jeżeli bowiem liczba $\beta^{rs}$ należy do ciała $K$, to przyjmując $\beta_1 = \beta^s$, wnosimy, że liczba $\beta_1^r$ będzie należała do $K$, zaś liczba $\beta^s$ do $K_1 = K(\beta_1)$.

Jeżeli wykładniki $q_1,q_2,\ldots,q_m$, są wszystkie mniejsze od $n$, to mówimy, że liczba $z$ daje się przedstawić za pomocą pierwiastników, których stopnie są mniejsze od $n$.

Jeżeli $q_1=q_2=\ldots=q_m=2$, to mówimy, że liczba $z$ daje się przedstawić za pomocą pierwiastników kwadratowych.

Jeżeli liczby $\alpha_1,\alpha_2,\ldots,\alpha_m$ są rzeczywiste, to mówimy, że liczba (rzeczywista) $z$ daje się przedstawić za pomocą pierwiastników rzeczywistych.

***Twierdzenie 11.*** *Dla każdej liczby naturalnej $n$ każdy z pierwiastków równania $z^n=1$ daje się przedstawić za pomocą pierwiastników, których stopnie są mniejsze od $n$.*

Dowód. Twierdzenie jest oczywiste dla $n=2$, gdyż pierwiastki równania $z^2=1$ są całkowite wymierne.

Załóżmy więc, że $n>2$ oraz że twierdzenie zachodzi dla wykładnika $n-1$.

Możemy oczywiście ograniczyć się do przypadku, kiedy $n$ jest liczbą pierwszą. W przeciwnym bowiem razie, oznaczając przez $p$ dzielnik pierwszy liczby $n$, mielibyśmy $n=pq_1$, gdzie $p<n$ i $q_1<n$; jeżeli teraz $z_1$ oznacza którykolwiek z pierwiastków równania $z^n=1$, to przyjmując $\alpha_1=z_1^{q_1}$, będziemy mieli $\alpha_1^p=z^{pq_1}=z_1^n=1$; zatem liczba $\alpha_1^p$ należy do ciała $\mathcal{R}$, zaś wobec $\alpha_1=z_1^{q_1}$ liczba $z_1^{q_1}$ należy do ciała $\mathcal{R}(\alpha_1)$. Liczba $z_1$ daje się więc przedstawić za pomocą pierwiastników, których stopnie są mniejsze od $n$.

W Teorii liczb dowodzi się, że jeżeli $n$ jest liczbą pierwszą, to istnieje taka liczba naturalna $g$, zwana *pierwiastkiem pierwotnym dla modułu $n$*, że reszty z dzielenia liczb:

$$1,\quad g,\quad g^2,\quad \ldots,\quad g^{n-2}$$

przez $n$ różnią się co najwyżej porządkiem od liczb $1,2,3,\ldots,n-1$.

Wystarczy oczywiście dalej brać pod uwagę tylko pierwiastki pierwotne równania $z^n=1$. Jak wiemy, są to pierwiastki równania:

$$z^{n-1}+z^{n-2}+z^{n-3}\ldots+z+1=0 \tag{27}$$

i jeżeli którykolwiek z nich oznaczymy przez $z_1$, to wszystkie są potęgami tego pierwiastka $z_1$ (Rozdział VI, § 8, str. 96, tw. 7). Możemy więc pierwiastki równania (27) ustawić w ciąg:

$$z_1,\quad z_1^2,\quad z_1^3,\quad \ldots,\quad z_1^{n-1},$$

albo — wobec określenia liczby $g$ — w ciąg:

$$z_1,\quad z_2=z_1^g,\quad z_3=z_2^g=z_1^{g^2},\quad \ldots,\quad z_{n-1}=z_{n-2}^g=z_1^{g^{n-2}}.$$



Niech $\varepsilon$ oznacza którykolwiek z pierwiastków $(n-1)$-go stopnia z jedności. Przyjmijmy:

$$f(z,\varepsilon)=z+\varepsilon z^g+\varepsilon^2 z^{g^2}+\ldots+\varepsilon^{n-2}z^{g^{n-2}}. \tag{28}$$

Otóż w myśl t. zw. *małego twierdzenia Fermata* liczba $g^{n-1}-1$ jest podzielna przez liczbę pierwszą $n$, a ponieważ $z_1^n=1$ i $\varepsilon^{n-1}=1$, więc $\varepsilon^{n-1}z^{g^{n-1}}=z_1$. Wzór (28) daje zatem wobec $z_2=z_1^g$:

$$\begin{aligned}\varepsilon f(z_2,\varepsilon)=\varepsilon f(z_1^g,\varepsilon)&=\varepsilon(z_1^{g^2}+\varepsilon z_1^{g^3}+\ldots+\varepsilon^{n-2}z_1^{g^{n-1}}g)\\&=\varepsilon z_1^{g^2}+\varepsilon^2 z_1^{g^3}+\ldots+\varepsilon^{n-2}z_1^{g^{n-2}}+z_1=f(z_1,\varepsilon)\end{aligned}$$

czyli

$$\varepsilon f(z_2,\varepsilon)=f(z_1,\varepsilon).$$

Podobnie wobec $z_3=z_2^g$ znajdujemy:

$$\varepsilon f(z_3,\varepsilon)=f(z_2,\varepsilon),$$

i dalej:

$$\varepsilon f(z_3,\varepsilon)=f(z_3,\varepsilon),\quad \ldots,\quad \varepsilon f(z_{n-2}\varepsilon)=f(z_{n-1},\varepsilon),$$

skąd wynika z łatwością wobec $\varepsilon^{n-1}=1$, że

$$[f(z_1,\varepsilon)]^{n-1}=[f(z_2,\varepsilon)]^{n-1}=\ldots=[f(z_{n-1},\varepsilon)]^{n-1}.$$

Wyrażenie $[f(z_1,\varepsilon)]^{n-1}=\dfrac{1}{n-1}\sum_{k=1}^{n-1}[f(z_k,\varepsilon)]^{n-1}$ jest więc wielomianem symetrycznym pierwiastków równania (27) i przeto (na mocy twierdzenia 2 Rozdziału IX § 3, str. 159) daje się wyrazić jako wielomian względem jego współczynników i liczby $\varepsilon$, czyli jako wielomian względem $\varepsilon$ o współczynnikach całkowitych

$$[f(z_1,\varepsilon)]^{n-1}=W(\varepsilon).$$

Stąd i z założenia, że twierdzenie 11 jest prawdziwe dla wykładnika $n-1$, wynika, że *liczba $f(z_1,\varepsilon)$ daje się przedstawić za pomocą pierwiastników, których stopnie są mniejsze od $n$*, gdyż liczba $\varepsilon$ może być w ten sposób przedstawiona.

Wynik ten jest słuszny dla każdego pierwiastka $\varepsilon$ równania $\varepsilon^{n-1}=1$; oznaczamy te pierwiastki przez $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{n-1}$.

Wobec (28) będzie dla $j=1,2,\ldots,n-1$:

$$f(z_1,\varepsilon_j)=z_1+\varepsilon_j z_1^g+\varepsilon_j^2 z_1^{g^2}+\ldots+\varepsilon_j^{n-2}z_1^{g^{n-2}};$$

zatem:

$$\sum_{j=1}^{n-1} f(z_1,\varepsilon_j)=(n-1)z_1+z_1^g\sum_{j=1}^{n-1}\varepsilon_j+z_1^{g^2}\sum_{j=1}^{n-1}\varepsilon_j^2+\ldots+z_1^{g^{n-2}}\sum_{j=1}^{n-2}\varepsilon_j^{n-2}. \tag{29}$$

Lecz — jak wiemy z twierdzenia 7 Rozdziału VI (§ 8, str. 96) — jeśli $\varepsilon$ jest pierwiastkiem pierwotnym $(n-1)$-go stopnia z jedności, to $\varepsilon_j=\varepsilon_1^j$ dla $j=1,2,\ldots,n-1$. Wobec tego, że $\varepsilon^{n-1}=1$ i że $\varepsilon_1^k\neq 1$ dla $k=1,2,\ldots,n-2$, wynika stąd, że

$$\sum_{j=1}^{n-1}\varepsilon_j^k=\sum_{j=1}^{n-1}\varepsilon_1^{jk}=\frac{\varepsilon_1^{k(n-1)}-1}{\varepsilon_1^k-1}=0 \quad \text{dla } k=1,2,\ldots,n-2.$$

Przeto wzór (29) daje:

$$\sum_{j=1}^{n-1} f(z_1,\varepsilon_j)=(n-1)z_1,$$

skąd:

$$z_1=\frac{1}{n-1}[f(z_1,\varepsilon_1)+f(z_1,\varepsilon_2)+\ldots+f(z_1,\varepsilon_{n-1})]. \tag{30}$$

Ponieważ — jak udowodniliśmy — liczba $f(z_1,\varepsilon)$, gdzie $\varepsilon^{n-1}=1$, daje się przedstawić za pomocą pierwiastników stopni mniejszych od $n$, wzór (30) dowodzi, że i liczba $z_1$ ma tę samą własność, c. b. d. o.

Zauważmy, że mimo prostoty dowodu twierdzenia 11, efektywne stosowanie tego twierdzenia nawet dla niewielkich $n$ doprowadza do bardzo żmudnych rachunków. Np. dla $n=11$ pierwiastkiem pierwotnym jest — jak łatwo sprawdzić — $g=2$, a przeto

$$f(z,\varepsilon)=z+\varepsilon z^2+\varepsilon^2 z^4+\varepsilon^3 z^8+\varepsilon^4 z^5+\varepsilon^5 z^{10}+\varepsilon^6 z^9+\varepsilon^7 z^7+\varepsilon^8 z^3+\varepsilon^9 z^6.$$

$[f(z,\varepsilon)]^{10}$ jest więc wielomianem stopnia 100 względem $z$.

Obliczenie wielomianu

$$W(\varepsilon)=[f(z_1,\varepsilon)]^{10}=\frac{1}{10}\sum_{k=1}^{10}[f(z_k,\varepsilon)]^{10}$$

jest zatem wysoce uciążliwe.



Z przeprowadzonego dowodu twierdzenia 11 wynika nadto następujące

***Twierdzenie 12.*** *Jeżeli $n$ jest liczbą pierwszą, to każdy pierwiastek $n$-go stopnia z jedności należy do ciała liczbowego, jakie otrzymamy, tworząc najprzód ciało liczbowe $\mathcal{R}(\varepsilon)$, gdzie $\varepsilon$ jest którymkolwiek pierwiastkiem pierwotnym $(n-1)$-go stopnia z jedności, a następnie dołączając do ciała $\mathcal{R}(\varepsilon)$ pewne pierwiastki $(n-1)$-go stopnia z pewnych $n-1$ liczb ciała $\mathcal{R}(\varepsilon)$.*

Z twierdzenia 12 wynika natychmiast

***Twierdzenie 13.*** *Jeżeli $n$ jest liczbą pierwszą postaci $2^k+1$, to każdy pierwiastek $n$-go stopnia z jedności daje się przedstawić za pomocą pierwiastników kwadratowych.*

Szczególne przypadki twierdzenia 13 dla $n=3, 5, 17$ otrzymaliśmy już na innej drodze w Rozdziale XI, § 1 (str. 199) i § 4 (str. 204).

## § 6. Układy liczb algebraicznie niezależnych.

O $m$ liczbach $z_1,z_2,\ldots,z_m$ (rzeczywistych lub zespolonych) mówimy, że są *algebraicznie niezależne*, jeżeli nie istnieje żaden nie będący tożsamościowo zerem wielomian $m$ zmiennych o współczynnikach wymiernych $W(x_1,x_2,\ldots,x_m)$ taki, iż $W(z_1,z_2,\ldots,z_m)=0$.

Oczywiście, jeżeli liczby $z_1,z_2,\ldots,z_m$ są algebraicznie niezależne, to przy wszelkim naturalnym $k$, gdzie $2\leqslant k\leqslant m$, każde $k$ spośród nich też są liczbami algebraicznie niezależnymi.

***Twierdzenie 13.*** *Jeżeli liczby $z_1,z_2,\ldots,z_m$ są algebraicznie niezależne, to żadna z nich nie jest liczbą algebraiczną.*

Dowód. Przypuśćmy, że np. $z_1$ jest liczbą algebraiczną, i niech $f(x)$ oznacza wielomian nieprzywiedlny o współczynnikach wymiernych, którego pierwiastkiem jest $z_1$. Przyjmując:

$$W(x_1,x_2,\ldots,x_m)=x_3x_2\ldots x_m f(x_1),$$

otrzymamy wielomian $m$ zmiennych $x_1,x_2,\ldots,x_m$ o współczynnikach wymiernych, nie będący tożsamościowo zerem i taki, iż $W(z_1,z_2,\ldots,z_m)=0$, wbrew założeniu, że liczby $z_1,z_2,\ldots,z_m$ są algebraicznie niezależne. Liczba $z_1$ nie może więc być algebraiczną, c. b. d. o.

Jak dowiódł v. Neumann[1]), każdej liczbie dodatniej $t$ można przyporządkować liczbę dodatnią $\nu(t)$ w ten sposób, aby dla każdego ciągu skończonego $t_1, t_2, \ldots, t_m$ różnych liczb dodatnich, liczby $\nu(t_1), \nu(t_2), \ldots, \nu(t_m)$ były algebraicznie niezależne. Przyporządkowanie to ustalił on przez wzór

$$\nu(t) = \sum_{n=0}^{\infty} \frac{2^{2^{\mathrm{E}(nt)}}}{2^{2^{n^2}}},$$

gdzie E oznacza „Entier" (p. str. 219).

Korzystając z tego wyniku, udowodnimy następujące

***Twierdzenie 14.*** *Każdemu zbiorowi $T$ liczb dodatnich można przyporządkować pewne ciało liczbowe $C(T)$ utworzone z liczb rzeczywistych, tak, aby różnym zbiorom liczb dodatnich odpowiadały zawsze różne ciała liczbowe.*

Dowód. Wystarczy w tym celu każdemu zbiorowi $T$ liczb dodatnich przyporządkować najmniejsze ciało liczbowe $C(T)$, zawierające każdą z liczb $\nu(t)$, gdzie $t$ należy do zbioru $T$.

Istotnie, okażemy, że jeżeli $T_1$ i $T_2$ są różnymi zbiorami liczb dodatnich, to ciała $C(T_1)$ i $C(T_2)$ są różne.

Skoro zbiory $T_1$ i $T_2$ są różne, to jeden przynajmniej z nich zawiera taką liczbę, której nie ma w drugim; niech np. $t$ należy do $T_2$, nie należąc do $T_1$. Ponieważ $t$ należy do $T_2$, więc z określenia ciała $C(T_2)$ wnosimy, że $\nu(t)$ należy do $C(T_2)$. Gdyby więc było $C(T_1)=C(T_2)$, to $\nu(t)$ musiałoby należeć do $C(T_1)$. Zatem wobec określenia ciała $C(T_1)$ byłoby:

$$\nu(t) = \frac{f(\nu(u_1), \nu(u_2), \ldots, \nu(u_m))}{g(\nu(u_1), \nu(u_2), \ldots, \nu(u_m))}, \tag{31}$$

gdzie $f$ i $g$ są wielomianami o współczynnikach wymiernych, zaś $u_1, u_2, \ldots, u_m$ różnymi liczbami zbioru $T_1$. Ze wzoru (31) wynika natychmiast, że między liczbami $\nu(t), \nu(u_1), \nu(u_2), \ldots, \nu(u_m)$ istniałaby zależność algebraiczna, co jest niemożliwe, gdyż liczby $t, u_1, u_2, \ldots, u_m$ są wszystkie różne: $t$ nie należy bowiem do $T_1$, zaś $u_1, u_2, \ldots, u_m$ są różnymi liczbami zbioru $T_1$.

Z twierdzenia 14 oraz z elementarnych twierdzeń Teorii mnogości można dalej z łatwością wysnuć

***Wniosek.*** *Różnych ciał liczbowych, utworzonych z liczb rzeczywistych, jest* $2^{2^{\aleph_0}}$, t. j. tyle, ile wszystkich zbiorów liczb rzeczywistych.

Mimo takiej obfitości różnych ciał liczbowych, utworzonych z liczb rzeczywistych, znalezienie choćby jednego nieprzeliczalnego ciała liczbowego, utworzonego z liczb rzeczywistych, ale nie ze wszystkich, uchodziło przez dłuższy czas za bardzo trudne. Świadczy o tym zagadnienie, postawione przez S. Mazurkiewicza w Tomie 1 czasopisma „Fundamenta Mathematicae" (1920 r.), str. 224, którego rozwiązanie znajduje się w pracy pośmiertnej M. Suslina, Fundamenta Mathematicae, Tom 4 (1924), str. 311-315.

[1]) J. v. Neumann, Mathematische Annalen, Tom 99 (1928), str. 134-141.

# ROZDZIAŁ XIV

# DOWODY NIEMOŻLIWOŚCI

## § 1. Niemożliwość przedstawienia pierwiastków wielomianu nieprzywiedlnego 3-go stopnia za pomocą pierwiastników kwadratowych.

Udowodnimy następujące

***Twierdzenie 1.*** *Pierwiastki równania o współczynnikach wymiernych*

$$z^3+pz+q=0, \tag{1}$$

*nie mającego pierwiastków wymiernych, nie dają się przedstawić za pomocą pierwiastników kwadratowych.*

Dowód. Przypuśćmy, że jeden z pierwiastków równania (1), np. $z_1$, daje się przedstawić za pomocą pierwiastników kwadratowych. Istnieje więc taki ciąg skończony liczb $\alpha_1, \alpha_2, \ldots, \alpha_m$, że $\alpha_1^2$ jest liczbą wymierną oraz że jeśli $R_0=\mathcal{R}$ i ogólnie $R_k=R_{k-1}(\alpha_k)$ dla $k=1,2,3,\ldots,m$, to $\alpha_k^2$ należy do $R_{k-1}$ dla $k=2,3,\ldots,m$, zaś $z_1$ należy do $R_m$. Możemy oczywiście założyć, że dla $k=1,2,\ldots,m$ liczba $\alpha_k$ nie należy do $R_{k-1}$ (t. j. że $R_k \neq R_{k-1}$) oraz że liczba $z_1$ nie należy do $R_{m-1}$.

Ponieważ $\alpha_m$ nie należy do $R_{m-1}$, więc $\alpha_m^2$ nie jest kwadratem liczby należącej do $R_{m-1}$, bowiem w razie $\alpha_m^2=u^2$ przy $u$ należącym do $R_{m-1}$ byłoby $\alpha_m=u$ lub $\alpha_m=-u$, a zatem $\alpha_m$ należałoby do $R_{m-1}$ wbrew założeniu. Ponieważ zaś $\alpha_m^2$ należy do $R_{m-1}$, więc w myśl twierdzenia 7 Rozdziału XIII (§ 3, str. 229) dwumian $x^2-\alpha_m^2$ jest nieprzywiedlny w ciele $R_{m-1}$, a że liczba $\alpha_m$ jest pierwiastkiem tego dwumianu, więc w myśl twierdzenia 8 tegoż Rozdziału (§ 3, str. 229) każda liczba ciała $R_m=R_{m-1}(\alpha_m)$, zatem i liczba $z_1$, daje się przedstawić w postaci $z_1=a+b\alpha_m$, gdzie liczby $a$ i $b$ należą do $R_{m-1}$. Lecz $z_1$ jest pierwiastkiem równania (1); mamy więc:

$$a^3+3ab^2\alpha_m^2+pa+q+(3a^2b+b^3\alpha_m^2+pb)\alpha_m=0. \tag{2}$$