Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Matematyczny
specjalność: matematyka nauczycielska

Aleksandra Mierzchała

Konstrukcje geometryczne - skrypt do zajęć.

Praca magisterska
napisana pod kierunkiem
dr hab. Jacka Świątkowskiego

Wrocław 2004

SPIS TREŚCI

WSTĘP

Praca została napisana na podstawie wykładu „Konstrukcje geometryczne i elementy teorii Galois" prowadzonego przez dr hab. Jacka Świątkowskiego.

Tematem skryptu jest pierwsza część wykładu dotycząca konstrukcji geometrycznych za pomocą cyrkla i linijki. Studiując kolejne rozdziały poznajemy sposoby rozstrzygania czy dane zadanie konstrukcyjne jest wykonalne za pomocą cyrkla i linijki. Skrypt zawiera m.in. odpowiedzi na słynne z historii matematyki zadania konstrukcyjne:

1. Zadanie Apoloniusza — konstrukcja okręgu stycznego do danych trzech okręgów.
2. Kwadratura koła — konstrukcja kwadratu o polu równym polu danego koła.
3. Podwojenie sześcianu — konstrukcja krawędzi sześcianu, którego objętość jest dwa razy większa od objętości danego sześcianu.
4. Trysekcja kąta — konstrukcja dzieląca dany kąt na trzy równe części.
5. Wielokąty foremne — konstrukcja n-kątów foremnych dla danego n.

Do każdego rozdziału dołączona jest lista zadań do samodzielnego rozwiązania przez studentów.

Studiowanie skryptu nie wymaga posiadania zaawansowanej wiedzy matematycznej, może poza znajomością liczb zespolonych, dlatego po uzupełnieniu tej luki jest on również dostępny dla uczniów liceum interesujących się matematyką.

ROZDZIAŁ I

Metoda algebraiczna w zadaniach konstrukcyjnych.

Metoda algebraiczna sprowadza zadanie konstrukcyjne do problemu skonstruowania jednego odcinka. Musimy zatem wyznaczyć długość tego odcinka, a następnie przeanalizować algebraicznie liczbę równą tej długości i rozstrzygnąć czy taki odcinek jest konstruowalny czy nie. Zobaczmy zastosowanie tej metody na przykładach.

Przykład 1.1

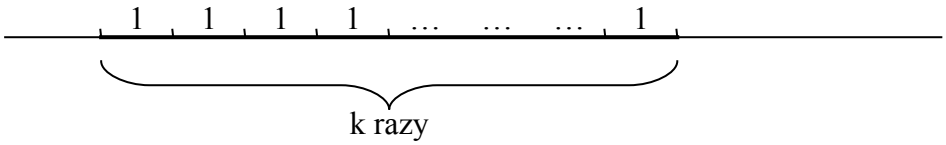
Zajmijmy się problemem kwadratury koła, czyli konstrukcją kwadratu o polu równym polu danego koła. Zadanie to sprowadza się do skonstruowaniu odcinka będącego bokiem szukanego kwadratu (ponieważ mając dany bok kwadratu umiemy skonstruować przy pomocy cyrkla i linijki kwadrat). Przyjmijmy, że dane koło ma promień długości 1. Zatem jego pole wynosi π. Szukany bok kwadratu nazwijmy *a*. Zatem pole kwadratu jest równe a^2. Zadanie mówi, że pola kwadratu i koła są równe, czyli $a^2 = \pi$. Wyliczając *a* otrzymujemy, że bok kwadratu ma długość $\sqrt{\pi}$. Jeżeli odcinek tej długości można skonstruować to zadanie konstrukcyjne jest wykonalne, w przeciwnym razie nie da się skonstruować kwadratu o danych własnościach. Do tego czy odcinek długości $\sqrt{\pi}$ jest konstruowalny wrócimy później.

Przykład 1.2

W zadaniu o podwojeniu sześcianu mamy skonstruować krawędź sześcianu, którego objętość jest dwa razy większa od objętości danego sześcianu. Przyjmijmy, że dany sześcian S_1 ma bok długości 1, a szukany sześcian S_2 bok długości *a*. Zatem ich objętości są odpowiednio równe $V(S_1) = 1^3 = 1, V(S_2) = a^3$. Z warunków zadania zapisujemy równość $V(S_2) = 2V(S_1)$, czyli $a^3 = 2$. Wyliczając *a* otrzymujemy, że krawędź sześcianu wynosi $\sqrt[3]{2}$. Tak jak w przykładzie 1.1 o tym czy konstrukcja sześcianu o danych własnościach jest wykonalna decyduje konstruowalność odcinka długości $\sqrt[3]{2}$. Do tego problemu również wrócimy później.

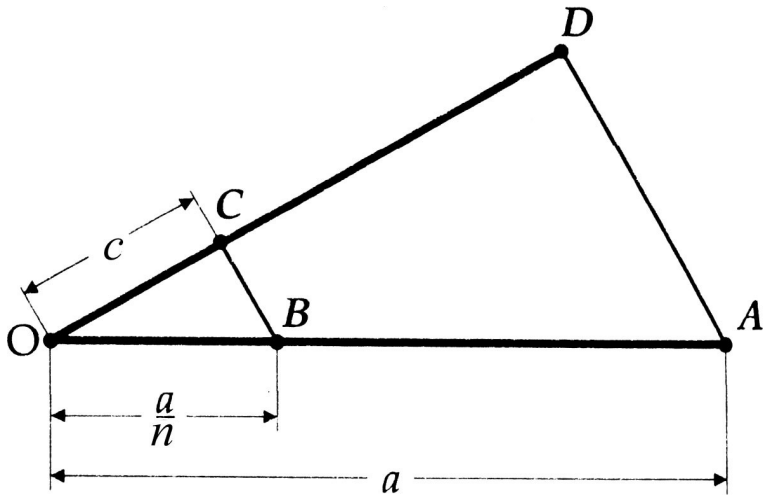
Spróbujmy teraz znaleźć długości odcinków, które można skonstruować za pomocą cyrkla i linijki wychodząc od danego odcinka długości 1.

1. Odkładając na prostej *k* razy odcinek jednostkowy możemy skonstruować odcinek o dowolnej długości naturalnej *k* (rys. 1).



Rysunek 1

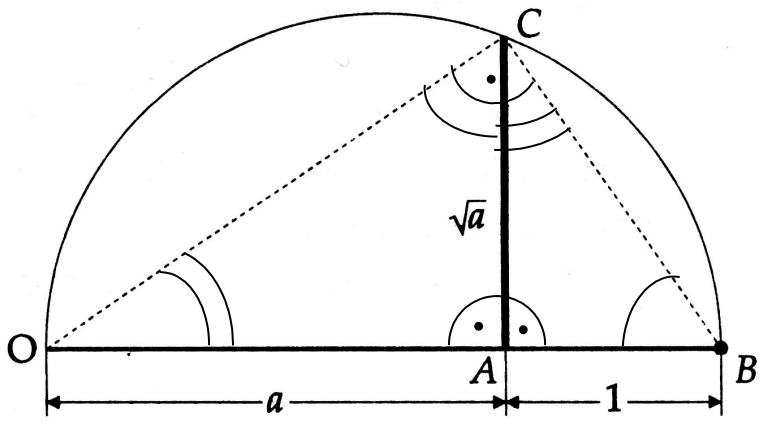
2. Każdy dany odcinek potrafimy podzielić na *m* równych części. Odcinek $\frac{a}{n}$ konstruujemy w następujący sposób (rys. 2): zaznaczamy na prostej odcinek $OA = a$ i przez punkt *O* prowadzimy dowolną inną prostą. Na tej drugiej prostej odmierzamy dowolny odcinek $OC = c$ i konstruujemy $OD = n \cdot c$. Łączymy punkty *A* i *D* i przez punkt *C* prowadzimy prostą równoległą do *AD*, która przetnie prostą *OA* w punkcie *B*. Trójkąty *OBC* i *OAD* są podobne; stąd $\frac{OB}{a} = \frac{OB}{OA} = \frac{OC}{OD} = \frac{1}{n}$ i $OB = \frac{a}{n}$.



Rysunek 2

Z punktów 1 i 2 wynika, że potrafimy skonstruować odcinek o dowolnej długości dodatniej wymiernej (czyli długości postaci *k/m*).

3. Mając dany odcinek długości *a*, możemy skonstruować odcinek długości $\sqrt{a}$. Na prostej odmierzamy *OA= a* i *AB= 1* (rys.3). Kreślimy okrąg, którego średnicą jest

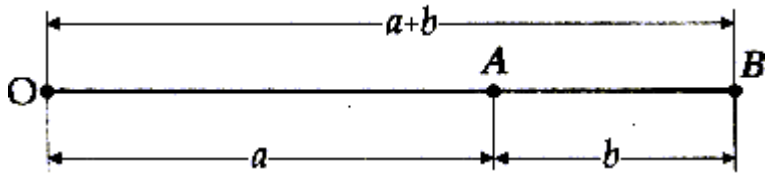


Rysunek 3

odcinek *OB*, i przez punkt *A* prowadzimy prostopadłą do *OB*, która przetnie okrąg w punkcie *C*. W trójkącie *OBC* kąt *C* jest prosty zgodnie z twierdzeniem geometrii elementarnej, głoszącym, że kąt wpisany w półkole jest kątem prostym. Stąd wynika, że kąt *OCA* jest równy kątowi *ABC*; trójkąty prostokątne *OAC* i *CAB* są podobne i mamy dla *x= AC*

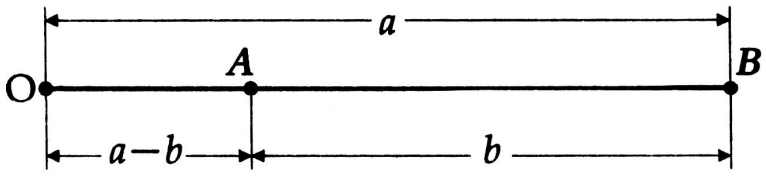
$\frac{x}{a} = \frac{1}{x}$, $x^2 = a$, $x = \sqrt{a}$.

4. Mając dane odcinki o długościach *a* i *b* możemy skonstruować odcinki długości *a+b* i *a-b*. Aby skonstruować *a+b* (rys.4), prowadzimy prostą i na niej za pomocą cyrkla zaznaczamy koło siebie odległości *OA=a* i *AB=b*. W takim razie *OB=a+b*.



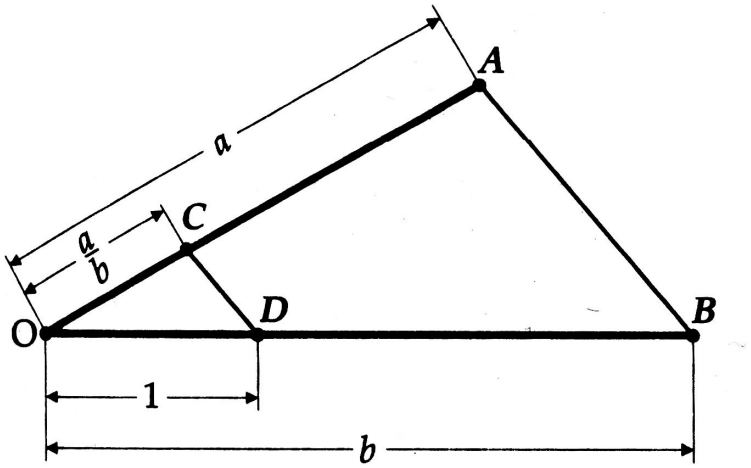
Rysunek 4

Podobnie dla otrzymania *a-b* (rys.5) zaznaczamy *OB=a AB=b*, ale tym razem AB odmierzamy w przeciwnym kierunku niż *OA*. Wobec tego *OA=a-b*.



Rysunek 5

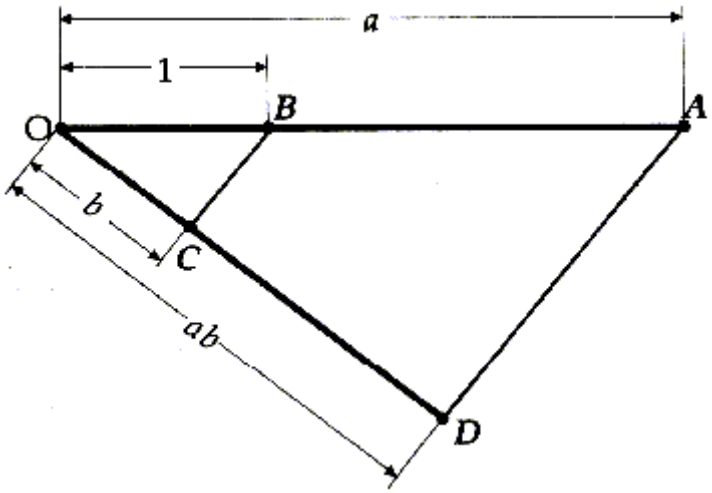
5. Mając dane odcinki o długościach *a* i *b* możemy skonstruować odcinki długości *ab* i $\frac{a}{b}$. Dla skonstruowania $\frac{a}{b}$ (rys.6) odmierzamy *OB=b* i *OA=a* na ramionach dowolnego kąta *O* i na boku *OB* odmierzamy *OD=1*. Przez punkt *D* prowadzimy prostą równoległą do *AB*, która przecina prostą *OA* w punkcie *C*.



Rysunek 6

Z twierdzenia Talesa: $\frac{b}{1} = \frac{a}{OC}$, skąd wyliczając *OC* otrzymujemy $OC = \frac{a}{b}$.

Konstrukcja *ab* jest pokazana na rys.7, gdzie prosta *AD* jest równoległą do *BC* poprowadzoną przez punkt *A*. Z twierdzenia Talesa: $\frac{1}{a} = \frac{b}{OD}$, skąd wyliczając *OD* otrzymujemy *OD = ab*.

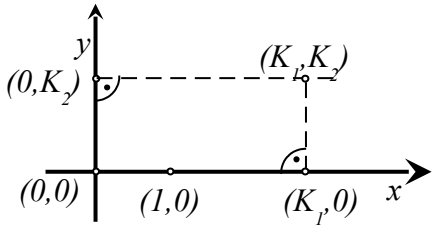


Rysunek 7

Oznaczmy symbolem **K** zbiór wszystkich liczb rzeczywistych dających się otrzymać z liczb wymiernych za pomocą skończonej liczby operacji sumy, różnicy, iloczynu, ilorazu oraz pierwiastka kwadratowego. Czyli do zbioru **K** należy np. liczba $\frac{\frac{3}{17}\cdot\sqrt{\frac{2}{7}}+\sqrt{8\frac{1}{2}}}{\sqrt{2-\frac{1}{3}\sqrt{2}}}$

Zauważmy, że zgodnie z naszymi rozważaniami na temat odcinków konstruowalnych (przy danym odcinku jednostkowym), dla dowolnej liczby *a* ze zbioru **K** potrafimy skonstruować odcinek długości |*a*| wychodząc od odcinka długości 1.

Zastanówmy się teraz, czy można skonstruować jeszcze jakieś inne liczby spoza zbioru **K** (wychodząc od odcinka jednostkowego). W tym celu rozważymy podobny problem na płaszczyźnie. Poszukajmy punktów, które potrafimy skonstruować mając dane punkty (0,0) oraz (1,0). Przyjrzyjmy się rysunkowi 8.



Rysunek 8

Niech K_1 i K_2 będą liczbami ze zbioru **K**. Wówczas punkt (K_1,K_2) jest konstruowalny za pomocą cyrkla i linijki jako punkt przecięcia prostej prostopadłej do osi x przechodzącej przez punkt $(K_1,0)$ i prostej prostopadłej do osi y przechodzącej przez punkt $(0, K_1)$. Zatem na

pewno potrafimy skonstruować wszystkie punkty ze zbioru $\mathbf{K}^2$, czyli wszystkie punkty o obu współrzędnych ze zbioru **K**.
Udowodnimy teraz następujące twierdzenie.

Twierdzenie 1.3

Mając dane punkty (0,0) i (1,0) nie można skonstruować za pomocą cyrkla i linijki żadnych innych punktów niż punkty z $\mathbf{K}^2$.

Dowód

Na płaszczyźnie za pomocą cyrkla i linijki możemy:

A) poprowadzić prostą przez dwa punkty, które są dane lub uprzednio skonstruowane;
B) poprowadzić okrąg o środku oraz promieniu danym lub uprzednio skonstruowanym;
C) wyznaczyć punkty przecięcia
   - dwóch prostych jak wyżej
   - prostej i okręgu jak wyżej
   - dwóch okręgów jak wyżej

Przyjmijmy, że punkty z $\mathbf{K}^2$ oraz odcinki o długościach z **K** mamy już skonstruowane. Sprawdźmy, czy da się skonstruować jakiekolwiek inne punkty lub odcinki. W tym celu uzasadnimy poniższe stwierdzenia.

Stwierdzenie 1.3.1

Prosta wyznaczona przez dwa punkty z $\mathbf{K}^2$ zadaje się równaniem $ax + by + c = 0$ o współczynnikach a, b, c ze zbioru **K**.

Znajdźmy ogólne równanie prostej wyznaczonej przez punkty $A = (a_1, b_1), B = (a_2, b_2)$ (współrzędne punktów to liczby ze zbioru **K**). Równanie prostej przechodzącej przez A i B wyraża się wzorem $y - b_1 = \frac{b_1 - b_2}{a_1 - a_2}(x - a_1)$.

Stąd otrzymujemy $(x\text{-}a_1)(b_1\text{-}b_2) = (y\text{-}b_1)(a_1\text{-}a_2)$. Zatem równanie ogólne prostej jest postaci: $(b - b_{21})x + (a_2 - a_1)y + a_1(b_2 - b_1) + b_1(a_1 - a_2) = 0$, gdzie współczynniki: $a = b_1 - b_2$, $b = a_2 - a_1$, $c = a_1(b_2 - b_1) + b_1(a_1 - a_2)$ należą do **K** (a, b należą do **K** jako różnice liczb z **K**,

natomiast *c* jako suma iloczynów liczby z **K** i różnicy liczb z **K**). Pokazaliśmy więc, że stwierdzenie 1.3.1 jest prawdziwe.

Stwierdzenie 1.3.2

Punkty przecięcia prostych zadanych równaniami o współczynnikach z **K** mają obie współrzędne w **K**.

Aby to pokazać musimy rozwiązać układ równań $\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \end{cases}$, gdzie $a_1x + b_1y - c_1 = 0$, $a_2x + b_2y - c_2 = 0$ są równaniami danych prostych. Zatem $a_1, b_1, c_1, a_2, b_2, c_2$ należą do zbioru **K** jako współczynniki tych prostych oraz $a_1b_2 - b_1a_2 \neq 0$ (proste nie są równoległe). Stosując wzory Cramera otrzymujemy rozwiązanie:

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} = \frac{c_1b_2 - b_1c_2}{a_1b_2 - b_1a_2}, \quad y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} = \frac{a_1c_2 - c_1a_2}{a_1b_2 - b_1a_2}$$

Liczby *x* i *y* przedstawiają się przy pomocy liczb z **K** i operacji iloczynu, różnicy oraz ilorazu. Zatem obie współrzędne *x* i *y* należą do zbioru **K**, co mieliśmy pokazać.

Stwierdzenie 1.3.3

Odległość pomiędzy dowolnymi dwoma punktami z $\mathbf{K}^2$ jest liczbą należącą do **K**.

Odległość dwóch punktów (a_1,b_1), (a_2,b_2) (gdzie $a_1, b_1, a_2, b_2,$ należą do **K**) wyraża się wzorem $\sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2}$. Otrzymaliśmy liczbę wyrażoną przez operacje sumy, różnicy, iloczynu i pierwiastka kwadratowego na liczbach z **K**. Stąd wynika, że odległość jest liczbą z **K**.

Stwierdzenie 1.3.4

Okrąg o środku w punkcie z $\mathbf{K}^2$ oraz o promieniu z **K** jest zadany równaniem o współczynnikach należących do **K**.

Zapiszmy równanie okręgu o środku $S = (a,b)$ i promieniu r (a, b, r należą do **K**). Jest ono postaci $(x-a)^2 + (y-b)^2 = r^2$. Równoważnie możemy je zapisać jako $x^2 - 2ax + y^2 - 2by + a^2 + b^2 - r^2 = 0$. Otrzymaliśmy równanie okręgu, którego współrzędne wyrażone są odpowiednio przez operacje sumy i różnicy liczb ze zbioru **K**. Czyli współczynniki są także liczbami należącymi do **K**.

Stwierdzenie 1.3.5

Rozwiązania równania kwadratowego $ax^2 + bx + c = 0$ o współczynnikach a, b, c ze zbioru **K** też należą do **K**.

Rozwiązaniami równania kwadratowego są liczby postaci $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Liczby te przedstawiają się przy pomocy liczb z **K** i operacji sumy, różnicy, iloczynu, ilorazu oraz pierwiastka kwadratowego. Zatem rozwiązania równania należą do **K**.

Stwierdzenie 1.3.6

Punkty przecięcia okręgu $x^2 + ax + y^2 + by + c = 0$ oraz prostej $px + qy + r = 0$, gdzie a, b, c, p, q, r należą do **K**, mają obie współrzędne z **K**, czyli należą do $\mathbf{K^2}$.

By znaleźć punkty przecięcia musimy rozwiązać układ równań:

$$\begin{cases} x^2 + ax + y^2 + by + c = 0 \\ px + qy + r = 0 \end{cases}.$$

Załóżmy, że $q \neq 0$ (pozostałe przypadki da się rozpatrzyć analogicznie). Wyznaczmy y z drugiego równania, czyli $y = -\frac{p}{q}x - \frac{r}{q}$. Wstawiając y do pierwszego równania otrzymujemy:

$x^2 + ax + \left(-\frac{p}{q}x - \frac{r}{q}\right)^2 + b\left(-\frac{p}{q}x - \frac{r}{q}\right) + c = 0$, stąd $x^2 + ax + \frac{p^2}{q^2}x^2 + 2\frac{pr}{q^2}x + \frac{r^2}{q^2} - \frac{pb}{q}x - \frac{br}{q} + c = 0$

i ostatecznie dostajemy równanie $\left(1 + \frac{p}{q}\right)x^2 + \left(a + \frac{2pr}{q^2} - \frac{pb}{q}\right)x + \left(c + \frac{r^2}{q^2} - \frac{br}{q}\right) = 0$.

Otrzymaliśmy równanie kwadratowe o współczynnikach z **K** (współczynniki powstały przez operacje sumy, różnicy, iloczynu i ilorazu na liczbach ze zbioru **K**). Na mocy stwierdzenia 1.3.5 rozwiązania tego równania należą do **K**. Współrzędna y punktu przecięcia też należy do **K** (jako różnica liczb z **K**). Zatem punkty przecięcia danego okręgu i prostej należą do $\mathbf{K^2}$.

Stwierdzenie 1.3.7

Punkty przecięcia okręgów $x^2 + ax + y^2 + by + c = 0$ oraz $x^2 + px + y^2 + qy + r = 0$, gdzie *a, b, c, p, q, r* to liczby ze zbioru **K**, należą do $\mathbf{K^2}$.

Szukamy punktów przecięcia danych okręgów rozwiązując układ równań:

$$\begin{cases} x^2 + ax + y^2 + by + c = 0 \\ x^2 + px + y^2 + qy + r = 0 \end{cases}.$$

Odejmując równania stronami otrzymujemy: $(a-p)x + (b-q)y + (c-r) = 0$. Czyli nasze zadanie sprowadza się do rozwiązania układu:

$$\begin{cases} (a-p)x + (b-q)y + (c-r) = 0 \\ x^2 + px + y^2 + qy + r = 0 \end{cases}.$$

Ze stwierdzenia 1.3.6 wiemy, że rozwiązania układu tej postaci należą do $\mathbf{K^2}$. Czyli punkt przecięcia danych okręgów należy do $\mathbf{K^2}$.

Uzasadniając powyższe stwierdzenia pokazaliśmy, że na płaszczyźnie przy danych punktach (0,0), (1,0) za pomocą cyrkla i linijki możemy skonstruować tylko punkty z $\mathbf{K^2}$ i odcinki o długościach z **K**, co kończy dowód twierdzenia 1.3.

W naszych rozważaniach możemy więc wyciągnąć wniosek.

Wniosek 1.4

Wychodząc od odcinka długości 1 nie można za pomocą cyrkla i linijki skonstruować żadnego odcinka o długości nie należącej do zbioru **K**.

Wprowadźmy zatem definicję.

Definicja 1.5

Zbiór **K** nazywamy zbiorem liczb konstruowalnych.

Do tej pory zajmowaliśmy się zagadnieniami konstruowalności odcinków przy danym odcinku długości 1. W niektórych zadaniach konstrukcyjnych mamy danych kilka innych

odcinków lub kilka punktów. Wtedy jeden z danych odcinków możemy przyjąć za jednostkowy. Zastanówmy się jakie odcinki lub punkty są wówczas konstruowalne.

Zdefiniujmy zbiór liczb konstruowalnych za pomocą zbioru, do którego należą odcinki o danych długościach.

Definicja 1.6

Dany jest zbiór liczb $A = \{a_1, \ldots, a_k\}$. Zbiorem liczb konstruowalnych za pomocą zbioru A nazywamy zbiór wszystkich liczb jakie można otrzymać z liczb wymiernych oraz z liczb $a_1, \ldots, a_k$ za pomocą operacji sumy, różnicy, iloczynu, ilorazu i pierwiastka kwadratowego. Zbiór ten oznaczamy symbolem **K(A)**.

Zauważmy, że jeżeli liczby $a_1, \ldots, a_k$ są konstruowalne to **K(A)** = **K**. Czyli żeby otrzymać liczby spoza zbioru **K** przynajmniej jedna z liczb $a_1, \ldots, a_k$ musi być niekonstruowalna.

Dla zbioru **K(A)** prawdziwe są poniższe twierdzenia.

Twierdzenie 1.7

Mając dane punkty (0,0), (1,0) oraz **K(B)**, gdzie $B = \{a_1, \ldots, a_k, b_1, \ldots, b_k\}$ możemy skonstruować wyłącznie punkty o obu współrzędnych z **K(B)**, czyli punkty ze zbioru **K(B)**×**K(B)**.

Twierdzenie 1.8

Za pomocą odcinków długości $1, a_1, \ldots, a_k$ można skonstruować wyłącznie odcinki o długościach należących do **K(A)**.

Uzasadnienia tych twierdzeń są analogiczne jak w przypadku zbioru **K**, więc nie będziemy ich już przytaczać.

Podsumowując, metoda algebraiczna pozwala nam, bez znajdowania konkretnych konstrukcji, rozstrzygać czy dane zadanie konstrukcyjne da się wykonać za pomocą cyrkla i linijki, czy nie. Konstruowalne są odcinki o długościach $|a|$, gdzie a należy do zbioru liczb

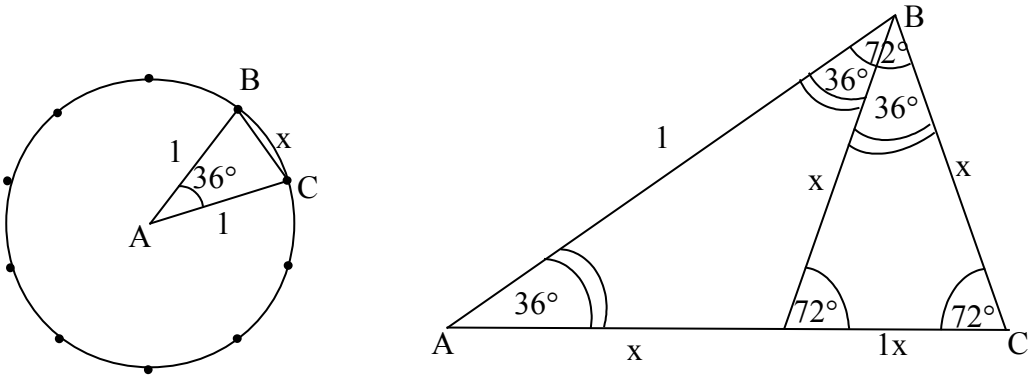
konstruowalnych. Udowodniliśmy również, że są to jedyne odcinki dające się skonstruować przy danym odcinku jednostkowym. Żeby otrzymać, odcinki o długościach spoza zbioru **K**, musimy mieć, danych kilka innych odcinków (zbiór *A*) przy czym przynajmniej jeden z nich musi być niekonstruowalny.

Na koniec, posługując się metodą algebraiczną, odpowiedzmy sobie czy wykonalne są konstrukcje dziesięciokąta foremnego i okręgu stycznego do danych trzech okręgów (tzw. zadanie Apoloniusza).

Przykład 1.9

Konstrukcja dziesięciokąta foremnego.

Narysujmy cyrklem na płaszczyźnie dowolny okrąg. Przyjmijmy, że jego promień wynosi 1 (rys.9). Rozważmy problem konstrukcji dziesięciokąta foremnego wpisanego w ten okrąg. Konstrukcja tego dziesięciokąta sprowadza się do konstrukcji odcinka *x* czyli boku dziesięciokąta. Mając dany odcinek *x* można skonstruować dziesięciokąt odmierzając od



Rysunek 9

dowolnego punktu na okręgu kolejne cięciwy o długości *x* aż do uzyskania wszystkich dziesięciu wierzchołków dziesięciokąta.

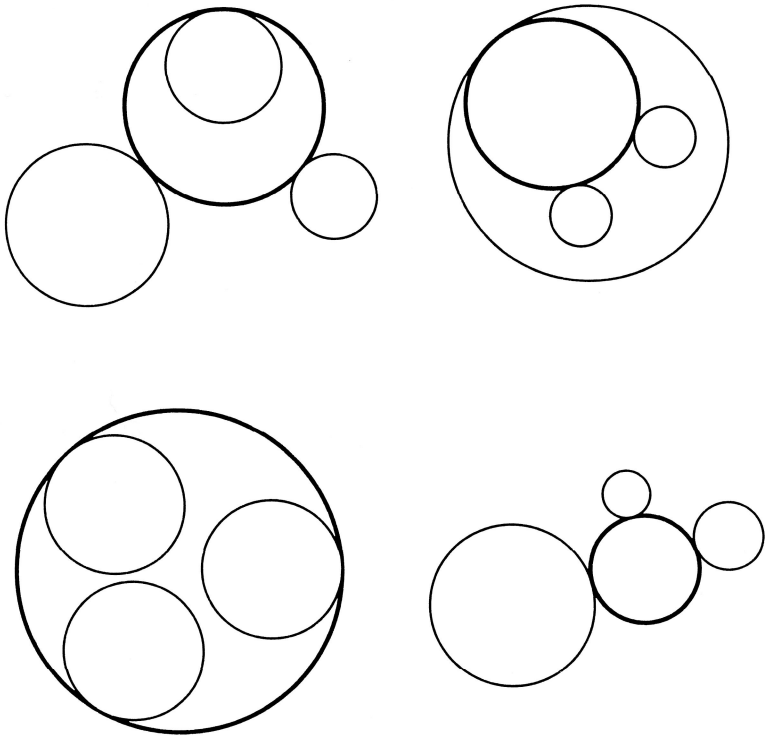
Wobec tego, że na odcinku *x* oparty jest kąt środkowy 36°, pozostałe dwa kąty trójkąta *OAB* wynoszą po 72°; dwusieczna kąta *B* dzieli trójkąt *OAB* na dwa trójkąty równoramienne, w których ramiona mają długość *x*. Promień koła zostaje zatem podzielony na dwa odcinki *x* i 1-*x*. Wobec tego, że trójkąt *OAB* jest podobny do trójkąta *ABC*, mamy $\frac{1}{x} = \frac{x}{1-x}$. Z tej proporcji otrzymujemy równanie $x^2 + x - 1 = 0$, którego rozwiązaniem jest $x = \frac{\sqrt{5}-1}{2}$ (drugie rozwiązanie odrzucamy ponieważ długość boku nie może być liczbą ujemną). Długość *x* jest liczbą konstruowalną, ponieważ wychodząc od odcinka jednostkowego umiemy

skonstruować odcinki długości: 2, 5, $\sqrt{5}$, $\sqrt{5}-1, \frac{\sqrt{5}-1}{2}$. Zatem konstrukcja dziesięciokąta foremnego jest wykonalna.

Przykład 1.10

Zadanie Apoloniusza polega na skonstruowaniu okręgu stycznego do danych trzech okręgów (jak na rysunku 10, gdzie pogrubiony okrąg jest szukanym okręgiem, który mamy skonstruować, pozostałe są dane).

Zajmijmy się przypadkiem w którym konstruowany okrąg jest styczny zewnętrznie do trzech danych okręgów (pozostałe przypadki rozstrzyga się analogicznie).



Rysunek 10

Obierzmy sobie na płaszczyźnie dwa punkty jeden niech będzie punktem (0,0), drugi punktem (1,0). Mamy dane trzy okręgi o środkach $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ i promieniach r_1, r_2, r_3 odpowiednio. Zatem zbiór danych liczb jest postaci $A = \{ x_1, y_1, x_2, y_2, x_3, y_3, r_1, r_2, r_3 \}$

Niech szukany okrąg S ma środek (x,y) i promień r. Przypomnijmy, że okręgi są styczne zewnętrznie wtedy i tylko wtedy, gdy odległość ich środków jest równa sumie ich promieni. Zapiszmy ten warunek dla naszego S i danych trzech okręgów. Otrzymujemy układ równań:

$$\begin{cases} (x-x_1)^2+(y-y_1)^2=(r+r_1)^2 \\ (x-x_2)^2+(y-y_2)^2=(r+r_2)^2 \\ (x-x_3)^2+(y-y_3)^2=(r+r_3)^2 \end{cases}$$

Obliczmy *x, y, r* i sprawdźmy czy należą do **K(A)**.

Po uporządkowaniu współczynników mamy:

$$\begin{cases} x^2+a_1x+y^2+b_1y=r^2+c_1r+d_1 \\ x^2+a_2x+y^2+b_2y=r^2+c_2r+d_2 \\ x^2+a_3x+y^2+b_3y=r^2+c_3r+d_3 \end{cases}$$

Współczynniki w układzie należą do **K(A)**. Odejmując od pierwszego równania trzecie otrzymamy: $(a_1-a_3)x+(b_1-b_3)y=(c_1-c_3)r+(d_1-d_3)$. Zapiszmy je w postaci: $m_1x+n_1y=p_1r+q_1$, gdzie m_1, n_1, p_1, q_1 należą do **K(A)**. Podobnie odejmując trzecie równanie od drugiego otrzymamy: $m_2x+n_2y=p_2r+q_2$, gdzie współczynniki należą do **K(A)**. Otrzymujemy równoważny układ równań:

$$\begin{cases} m_1x+n_1y=p_1r+q_1 \\ m_2x+n_2y=p_2r+q_2 \\ x^2+a_3x+y^2+b_3y=r^2+c_3r+d_3 \end{cases}$$

Potraktujmy r jako parametr i rozwiążmy układ równań liniowych:

$$\begin{cases} m_1x+n_1y=p_1r+q_1 \\ m_2x+n_2y=p_2r+q_2 \end{cases}$$

Zajmijmy się przypadkiem w którym środki okręgów nie leżą na jednej prostej. Wtedy wyznacznik główny powyższego układu jest niezerowy, czyli $m_1n_2-n_1m_2\neq 0$. Zatem rozwiązaniem układu jest :

$$x=\frac{\begin{vmatrix} p_1r+q_1 & n_1 \\ p_2r+q_2 & n_2 \end{vmatrix}}{\begin{vmatrix} m_1 & n_1 \\ m_2 & n_2 \end{vmatrix}}=\frac{(p_1r+q_1)n_2-(p_2r+q_2)n_1}{m_1n_2-n_1m_2}=s_1+t_1r,$$

podobnie $y=s_2+t_2r$.

Współczynniki s_1, s_2, t_1, t_2 należą do **K(A)**. Podstawiając rozwiązania *x* i *y* do trzeciego równania otrzymujemy:

$$(s_1 + t_1 r)^2 + a_3(s_1 + t_1 r) + (s_2 + t_2 r)^2 + b_3(s_2 + t_2 r) = r^2 + c_3 r + d_3$$

Po uporządkowaniu dostajemy równanie w postaci: $\mathrm{Pr}^2 + Qr + S = 0$, gdzie *P,Q,S* należą do **K(A)**. Stąd $r = \frac{-Q+\sqrt{Q^2-4PS}}{2P}$, jest liczbą ze zbioru **K(A)**. Podobnie jak $x = s_1 + t_1 r$ i $y = s_2 + t_2 r$. Czyli szukany okrąg jest konstruowalny.

ZADANIA

Zad.1.1. Mając dany odcinek jednostkowy, skonstruuj odcinki o długościach: $\frac{1}{5}, \frac{11}{17}, \sqrt{2}, \sqrt{2\frac{1}{3}}, \quad \sqrt{1+\sqrt{2}}, \sqrt{\sqrt{5}-\sqrt{3}}, \frac{2+\sqrt{7}}{\sqrt{3}-\sqrt{2}}, \sqrt[8]{2}$. Opisz schematycznie, za pomocą rysunków, etapy wykonywania tych konstrukcji.

Zad.1.2. Mając dane punkty (0, 0) i (1, 0) skonstruuj punkty $\left(2\frac{2}{3}, 1\frac{1}{7}\right), \left(-5\frac{1}{2}, \frac{1}{2}+\frac{1}{3}\sqrt{5}\right)$.

Zad.1.3. Dany jest odcinek długości 1. Skonstruuj kwadrat, dla którego suma obwodu i pola wynosi 4.

Zad.1.4. Skonstruuj trójkąt równoramienny mając dany jego obwód $2p$ oraz wysokość $h=1$.

Zad.1.5. Dane są odcinki a,b,c,d,e,f. Bez posługiwania się odcinkiem jednostkowym skonstruuj odcinki o następujących długościach:

$\frac{ab}{c}, \frac{2a^2}{3b}, \frac{abc}{df}, \frac{a^2+2bc}{d}, \frac{ab}{3c+d}, \frac{a^2+2bc}{d+f}, \sqrt{\frac{1}{2}ab}, \sqrt{a^2+b^2}, \sqrt{c^2+d^2}, \sqrt{a^2+bc}, \sqrt{a^2+3b^2},$

$\sqrt{ab-\sqrt{2}cd}, a\sqrt{2}, a\sqrt{7}, a\sqrt{3}/\left(1+\sqrt{5}\right), \sqrt[4]{abcd}, \sqrt[4]{a^4-b^4}, \sqrt[4]{2a^4+3b^4}$.

Zad.1.6. Dane są odcinki *a* i *b*. Skonstruuj dwa odcinki

(a) których suma jest równa *a*, zaś iloczyn jest równy b^2;

(b) których różnica jest równa *a*, zaś iloczyn jest równy b^2.

Zad.1.7. Dane są punkty *A* i *B* których współrzędne są liczbami konstruowalnymi. Uzasadnij, że jeżeli *O* jest początkiem układu współrzędnych, to następujące liczby

(a) długość odcinka *AB*;

(b) cosinus kąta *AOB*;

(c) pole trójkąta *AOB*;

są liczbami konstruowalnymi.

Zad.1.8. Dany jest kąt α, którego cosinus jest liczbą konstruowalną. Uzasadnij, że następujące liczby są liczbami konstruowalnymi:

(a) $\sin\alpha$

(b) $\cos\frac{1}{2}\alpha$

(c) długość cięciwy okręgu jednostkowego opartej na kącie środkowym α;

Zad.1.9. Większy z boków danego prostokąta podziel konstrukcyjnie na takie dwie części, tak, by suma pól kwadratów zbudowanych na tych dwóch częściach była równa polu tego prostokąta.

Zad.1.10. Podaj konstrukcję *złotego podziału* danego odcinka. Przypomnijmy, że punkt C odcinka AB dzieli go w złotym stosunku, jeśli $AC : CB = AB : AC$. Wskazówka: przyjmijmy, że dany odcinek ma długość 1,dokonaj algebraicznych wyliczeń i naszkicuj wynikającą z nich konstrukcję.

Zad.1.11. (a) Uzasadnij obliczając kąty i znajdując pomocnicze trójkąty równoramienne, że jeśli w pięciokącie foremnym poprowadzimy dwie przecinające się przekątne, to na każdej z nich otrzymamy odcinek równy bokowi tego pięciokąta.

(b) Udowodnij, że punkt przecięcia dwóch przekątnych w pięciokącie foremnym dzieli każdą z nich w złotym stosunku.

(c) Podaj konstrukcję pięciokąta foremnego opartą na konstrukcji złotego podziału odcinka.

Zad.1.12. (a) Uzasadnij, że jeśli c' jest cięciwą w okręgu jednostkowym opartą na kącie środkowym dwa razy mniejszym niż cięciwa c, to $c' = \sqrt{2 - \sqrt{4 - c^2}}$.

(b) Wyprowadź indukcyjnie wzór na długość boku 2^n-kąta oraz $3 \cdot 2^n$-kąta foremnego wpisanego w okrąg jednostkowy. Uzasadnij, że długość ta jest dla każdego $n \in N$ liczbą konstruowalną. Czy można było spodziewać się tego bez obliczeń?

Zad.1.13. Posługując się metodą algebraiczną uzasadnij, że następujące konstrukcje są wykonalne za pomocą cyrkla i linijki:

(a) konstrukcja kwadratu o polu równym polu danego trójkąta (kwadratura trójkąta);

(b) konstrukcja koła o polu równym sumie pól dwóch danych kół (koło uznajemy za dane, jeśli dane są jego środek oraz promień):

(c) podział danego trójkąta na dwie części o równych polach za pomocą prostej równoległej do wybranej podstawy.

Ustal oznaczenia przyjmując jeden z danych odcinków za jednostkowy. Sprowadź problem do pytania o konstruowalność pewnego pojedynczego odcinka. Wyliczając długość tego odcinka uzasadnij, że jest on możliwy do skonstruowania.

Zad.1.14. Dane są punkty (0, 0) oraz (1, 0). Wylicz algebraicznie, że konstrukcja okręgu stycznego do okręgu $x^2 + y^2 = 1$ i przechodzącego przez punkty $A(2, 1)$ i $B(3, 2)$ jest

wykonalna. Wskazówka: wylicz, że współrzędne środka oraz promień szukanego okręgu są liczbami konstruowalnymi.

ROZDZIAŁ II

Ciała liczbowe i rozszerzenia kwadratowe.

Definicja 2.1

Ciałem liczbowym L nazywamy dowolny zbiór liczb zespolonych zamknięty ze względu na działania dodawania, odejmowania, mnożenia i dzielenia (przez liczby różne od zera). Ponadto zakładamy, że 0 i 1 należą do L.

Definicja ta oznacza, że jakiekolwiek działania wymierne zastosowane do dwóch lub więcej elementów ciała, dają liczbę tegoż ciała.

Aby stwierdzić czy dany zbiór L jest ciałem liczbowym wystarczy więc sprawdzić czy spełnione są poniższe warunki:

(1) $0 \in L, \quad 1 \in L$

(2) jeśli $a, b \in L$, to $a + b \in L$, $ab \in L$,

(3) jeśli $a \in L$, to $-a \in L$

(4) jeśli $a \in L$ i $a \neq 0$, to $\frac{1}{a} \in L$.

Zauważmy, że z powyższej charakteryzacji ciała liczbowego wynika poniższe stwierdzenie.

Stwierdzenie 2.2

Każde ciało liczbowe L zawiera wszystkie liczby wymierne.

Dowód

Wiemy, że 0 i 1 są elementami ciała L. Ponieważ L jest zamknięty na działanie dodawania, to 1+1, (1+1)+1, $\cdots$ też należą do L. Zatem zbiór liczb naturalnych $\{1, 2 = 1 + 1, 3 = (1 + 1) + 1, \ldots\}$ zawiera się w L. Z warunku (3) wynika, że elementy przeciwne do elementów ciała L też należą do L. Pokazaliśmy już, że elementami ciała L są liczby naturalne, więc na mocy (3) liczby do nich przeciwne, czyli $-1, -2, -3, \ldots$ należą do L. Zatem

zbiór liczb całkowitych $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ zawiera się w *L*. Pozostaje nam jeszcze uzasadnić, że zbiór liczb wymiernych zawiera się w *L*. Liczby wymierne definiujemy jako ułamki nieskracalne postaci $\frac{p}{q}$, gdzie *p* i *q* są całkowite. Ponieważ ciało *L* jest zamknięte na operację dzielenia, więc ilorazy $\frac{p}{q}$ elementów *p, q* z ciała *L* należą do *L*. Zatem zbiór liczb wymiernych zawiera się w *L*.

Pamiętamy, że liczby wymierne, liczby rzeczywiste i liczby zespolone tworzą ciała.

Przyjrzyjmy się teraz przykładowi innego zbioru tworzącego ciało liczbowe.

Przykład 2.3

Dany mamy zbiór $Q(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in Q\}$. Sprawdźmy, czy tak zdefiniowany zbiór jest ciałem liczbowym. W tym celu zobaczmy czy spełnione są warunki (1)-(4).

(1) 0 jest elementem $Q(\sqrt{2})$ ponieważ przedstawia się w postaci $a + b\sqrt{2}$, gdzie *a* i *b* są zerami. Podobnie 1 należy do $Q(\sqrt{2})$ dla $a = 1$ i $b = 0$.

(2) Weźmy dwa elementy zbioru $Q(\sqrt{2})$ $a + b\sqrt{2}$ oraz $c + d\sqrt{2}$ ($a, b, c, d \in Q$). Sprawdźmy, czy ich suma i iloczyn należą do $Q(\sqrt{2})$. Dla sumy $(a + b\sqrt{2}) + (c + d\sqrt{2})$ mamy postać $(a + c) + (b + d\sqrt{2}) = p_1 + q_1\sqrt{2}$, gdzie $p_1 = a + c,\ q_1 = b + d$ są wymierne, więc suma należy do $Q(\sqrt{2})$.

Natomiast iloczyn $(a + b\sqrt{2})(c + d\sqrt{2})$ przedstawia się w postaci $(ac + 2bd) + (ad + bc)\sqrt{2} = p_2 + q_2\sqrt{2}$, gdzie $p_2 = ac + 2bd,\ q_2 = ad + bc$ są wymierne, więc iloczyn również należy do $Q(\sqrt{2})$.

(3) Element przeciwny $-(a + b\sqrt{2})$ postaci $-a + (-b)\sqrt{2} = p + q\sqrt{2}$, gdzie $p = -a,\ q = -b$ są wymierne należy do $Q(\sqrt{2})$.

(4) Element odwrotny $\frac{1}{a+b\sqrt{2}}$ po usunięciu niewymierności z mianownika jest postaci $\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}=p+q\sqrt{2}$ gdzie $p=\frac{a}{a^2-2b^2}$, $q=\frac{-b}{a^2-2b^2}$ są wymierne, więc także należy do $Q\left(\sqrt{2}\right)$.

Warunki (1)-(4) są spełnione, zatem zbiór $Q\left(\sqrt{2}\right)$ jest ciałem liczbowym.

Przykład 2.3 ma następujące uogólnienie.

Przyjmijmy za dane ciało liczbowe *F*. Weźmy dodatni element *a* ciała *F* taki, że $\sqrt{a}$ nie należy do *F*. Dla takich *F* i *a* prawdziwy jest poniższy lemat.

Lemat 2.4

Zbiór $F\left(\sqrt{a}\right)\coloneqq\left\{x+y\sqrt{a}:x,y\in F\right\}$ jest ciałem liczbowym.

Dowód

Tak jak w przykładzie 2.3 sprawdzamy, czy zbiór spełnia warunki (1)-(4). Warunki (1)-(3) pomijamy (uzasadnia się je tak samo jak w przykładzie 2.3), rozpatrzmy jedynie warunek (4). Element odwrotny $\frac{1}{x+\sqrt{a}}$ mnożymy przez $\frac{x-\sqrt{a}}{x-\sqrt{a}}$, otrzymujemy wtedy postać $\frac{x}{x^2-ay^2}+\frac{-y}{x^2-ay^2}\sqrt{a}$. Ponieważ $x,y,a\in F$, to również liczby $\frac{x}{x^2-ay^2},\frac{-y}{x^2-ay^2}$ należą do *F*. Pozostaje jeszcze sprawdzić, czy $x-y\sqrt{a}\neq 0$. Gdyby $x-y\sqrt{a}=0$, to $x=y\sqrt{a}$, czyli $\sqrt{a}=\frac{x}{y}$, ale wtedy $\sqrt{a}$ byłby elementem *F,* wbrew wcześniejszemu założeniu. Zatem $x-y\sqrt{a}$ nie może być zerem. Zbiór $F\left(\sqrt{a}\right)$ spełnia warunki (1)-(4), więc jest ciałem liczbowym.

Dla tak zdefiniowanego ciała $F\left(\sqrt{a}\right)$ możemy wprowadzić definicję.

Definicja 2.5

Ciało postaci $F\left(\sqrt{a}\right)$ nazywamy rozszerzeniem kwadratowym ciała *F*.

Na mocy definicji 2.5 zbiór $Q(\sqrt{2})$ zdefiniowany w przykładzie 2.3 możemy nazwać rozszerzeniem kwadratowym ciała liczb wymiernych o $\sqrt{2}$.

W zagadnieniu konstruowalności liczb pojęcie rozszerzenia kwadratowego daje nam nowy argument w rozstrzyganiu czy dana liczba jest konstruowalna, czy nie jest. Świadczy o tym poniższe twierdzenie.

Twierdzenie 2.6

Liczba p jest konstruowalna wtedy i tylko wtedy, gdy istnieje ciąg rozszerzeń kwadratowych $Q = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_n$ taki, że p należy do F_n.

Dowód

$(\Leftarrow)$ Załóżmy, że $p \in F_n$. Wówczas p jest postaci $a + b\sqrt{c}$, gdzie $a, b, c \in F_{n-1}$. Postępując podobnie z liczbami a, b, c i z dalszymi liczbami dostaniemy ostatecznie wyrażenie przedstawiające p za pomocą liczb wymiernych oraz operacji sumy, różnicy, iloczynu, ilorazu i pierwiastka kwadratowego. Stąd p jest konstruowalna.

$(\Rightarrow)$ Załóżmy, że p jest konstruowalna. Wtedy p wyraża się za pomocą liczb wymiernych oraz operacji sumy, różnicy, iloczynu, ilorazu i pierwiastka kwadratowego. Wykonywanie powyższych działań wymiernych nie wyprowadza nas poza ciało. Natomiast wykonywanie operacji pierwiastka kwadratowego (o ile wyprowadza poza dotychczasowe ciało) sprowadza się do przejścia do większego ciała, będącego rozszerzeniem kwadratowym poprzedniego ciała. Stąd istnieje ciąg rozszerzeń dla liczby p.

Obie implikacje zachodzą, więc twierdzenie jest prawdziwe.

W kolejnych przykładach znajdziemy ciągi rozszerzeń kwadratowych dla danych liczb konstruowalnych.

Przykład 2.7

Dana jest liczba $p = \dfrac{1+\sqrt{2}}{2-\sqrt{3}}$. Szukamy rozszerzeń kwadratowych dla liczby p. Jako F_0 przyjmujemy Q. Sprawdźmy czy p należy do Q.

Załóżmy, że p jest wymierna. Wtedy dla $p=\frac{1+\sqrt{2}}{2-\sqrt{3}}$ mamy, $1+\sqrt{2}=2p-\sqrt{3}p$, co równoważnie możemy zapisać jako $\sqrt{2}+\sqrt{3}p=2p-1$. Podnosząc obustronnie do kwadratu otrzymujemy $2+2\sqrt{6}p+3p^2=4p^2-4p+1$. Przekształcamy równanie do postaci $\sqrt{6}=\frac{p^2-4p-1}{2p}$. Dostaliśmy przedstawienie $\sqrt{6}$ w postaci ilorazu liczb wymiernych. Wtedy $\sqrt{6}$ także jest liczbą wymierną, sprzeczność z niewymiernością liczby $\sqrt{6}$. Czyli p nie należy do F_0.

Rozszerzamy więc $F_0=Q$ o liczbę $\sqrt{2}$. Otrzymujemy rozszerzenie $F_1=Q(\sqrt{2})$. Sprawdźmy teraz czy p należy do F_1. Gdyby p była elementem F_1, to ponieważ F_1 jest ciałem odwrotność liczby p równa $\frac{2-\sqrt{3}}{1+\sqrt{2}}$ też należałaby do F_1, tak jak i liczba $2-\sqrt{3}=\frac{2-\sqrt{3}}{1+\sqrt{2}}\cdot(1+\sqrt{2})$. Wtedy też liczba $\sqrt{3}=(2-\sqrt{3})+2$ należałaby do F_1. Gdyby $\sqrt{3}$ należał do F_1, to byłby postaci $a+b\sqrt{2}$, gdzie *a, b* są wymierne czyli $\sqrt{3}=a+b\sqrt{2}$. Podnosząc obustronnie do kwadratu otrzymujemy $3=a^2+2b^2+2ab\sqrt{2}$, czyli układ $\begin{cases}a^2+2b^2=3\\2ab=0\end{cases}$ powinien mieć wymierne rozwiązanie. Z drugiego równania wynika, że $a=0$ lub $b=0$. Podstawiając $a=0$ lub $b=0$ do pierwszego równania dochodzimy do sprzeczności. Zatem układ nie ma rozwiązania, więc $\sqrt{3}$ nie może należeć do F_1, tak jak i liczba *p.*

Szukamy innego rozszerzenia do którego będzie należeć *p*. Rozszerzmy $F_1=Q(\sqrt{2})$ o liczbę $\sqrt{3}$, otrzymujemy $F_2=F_1(\sqrt{3})$**.** Zauważmy**,** że p należy do F_2 jako iloraz liczb z F_2 (liczba $1+\sqrt{2}$ należy do F_1, więc tym bardziej do F_2, liczba $2-\sqrt{3}$ jest liczbą postaci $a+b\sqrt{3}$, gdzie *a, b* należą do F_1, stąd także należy do F_2). Znaleźliśmy ciało F_2 do którego należy dana liczba *p*.

Zatem ciąg rozszerzeń kwadratowych liczby *p* jest postaci $Q=F_0\subset F_1\subset F_2$.

Przykład 2.8

Dla liczby $q=\sqrt{2}+\sqrt{1+\sqrt{2}}$ szukamy ciągu rozszerzeń kwadratowych. Tak jak poprzednio za F_0 przyjmujemy *Q*. Przeprowadzając analogiczne rozumowanie jak w przykładzie 2.7 pokazujemy, że *q* nie jest wymierna.

Rozszerzamy więc $F_0=Q$ o $\sqrt{2}$ otrzymujemy rozszerzenie $F_1=Q\left(\sqrt{2}\right)$. Sprawdźmy czy *q* należy do F_1. Gdyby *q* należało do ciała F_1, to liczba $\sqrt{1+\sqrt{2}}=q-\sqrt{2}$ też. Wtedy $\sqrt{1+\sqrt{2}}$ byłby postaci $a+b\sqrt{2}$, gdzie *a, b* są wymierne, czyli $\sqrt{1+\sqrt{2}}=a+b\sqrt{2}$. Podnosząc obustronnie do kwadratu otrzymujemy $1+\sqrt{2}=a^2+2b^2+2ab\sqrt{2}$, czyli układ $\begin{cases}a^2+2b^2=1\\2ab=1\end{cases}$ powinien mieć wymierne rozwiązanie. Z drugiego równania wyznaczmy $b=\frac{1}{2a}$ i wstawiamy do pierwszego równania. Stąd otrzymujemy równanie $a^2+\frac{1}{2a^2}=1$ i przekształcamy je do postaci $a^4-a^2+\frac{1}{2}=0$. Podstawiamy $t=a^2$ do równania $a^4-a^2+\frac{1}{2}=0$, wtedy jest ono postaci $t^2-t+\frac{1}{2}=0$. Obliczając wyróżnik otrzymanego trójmianu kwadratowego stwierdzamy, że takie równanie nie ma rozwiązań rzeczywistych, a więc tym bardziej wymiernych. Zatem liczba $\sqrt{1+\sqrt{2}}$ nie należy do F_1, podobnie jak *q*.

Rozszerzamy teraz ciało $F_1=Q\left(\sqrt{2}\right)$ o liczbę $\sqrt{1+\sqrt{2}}$. Otrzymujemy $F_2=F_1\left(\sqrt{1+\sqrt{2}}\right)$. Zauważmy, że liczba *q* należy do F_2 jako suma liczb z F_2. Znaleźliśmy więc ciało F_2, którego elementem jest *q*.

Stąd ciąg rozszerzeń kwadratowych liczby *q* jest postaci $F_0\subset F_1\subset F_2$.

Wróćmy teraz do zagadnienia podwojenia sześcianu z przykładu 1.2. Do zdecydowania czy to zadanie jest wykonalne za pomocą cyrkla i linijki brakuje nam wiedzy na temat konstruowalności liczby $\sqrt[3]{2}$. Udowodnijmy zatem poniższe twierdzenie.

Twierdzenie 2.9

$\sqrt[3]{2}$ nie jest liczbą konstruowalną.

Dowód

Przede wszystkim $\sqrt[3]{2}$ nie jest liczbą wymierną (dowód tego faktu zostawiamy jako ćwiczenie). Załóżmy więc nie wprost, że $\sqrt[3]{2}$ jest konstruowalny. Wówczas istnieje ciąg rozszerzeń kwadratowych $Q = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n$ taki, że $\sqrt[3]{2}$ należy do F_n. Załóżmy ponadto, że F_n jest pierwszym ciałem w tym ciągu zawierającym $\sqrt[3]{2}$ (czyli $\sqrt[3]{2}$ nie należy do F_{n-1}). Przyjmijmy, że $F_n = F_{n-1}\left(\sqrt{a}\right)$, gdzie *a* należy do F_{n-1} i $\sqrt{a}$ nie należy do F_{n-1}. Możemy więc zapisać, że $\sqrt[3]{2} = x + y\sqrt{a}$ dla pewnych *x,y* z F_{n-1}. Podnosząc obustronnie do trzeciej potęgi otrzymujemy $2 = \left(x + y\sqrt{a}\right)^3 = \left(x^3 + 3xy^2a\right) + \left(3x^2y + ay^3\right)\sqrt{a}$. Zauważmy, że współczynnik $3x^2y + ay^3$ musi być równy zero, bo w przeciwnym wypadku $\sqrt{a} = \dfrac{2 - \left(x^3 + 3xy^2a\right)}{3x^2y + ay^3}$ i $\sqrt{a}$ należałby do F_{n-1} wbrew założeniu. Zatem $3x^2y + ay^3 = 0$ oraz $x^3 + 3xy^2a = 2$.

Weźmy liczbę $x - y\sqrt{a}$. Ponieważ *y* nie jest zerem (gdyby *y* był zerem to $\sqrt[3]{2}$ byłby elementem F_{n-1} wbrew założeniu), więc liczby $x - y\sqrt{a}$ i $x + y\sqrt{a}$ są różne. Obliczając $\left(x - y\sqrt{a}\right)^3$ otrzymujemy $\left(x^3 + 3xy^2a\right) - \left(3x^2y + ay^3\right)\sqrt{2} = 2 - 0\sqrt{2} = 2$. Pokazaliśmy zatem, że $\left(x - y\sqrt{a}\right)^3 = 2$ i $\left(x + y\sqrt{a}\right)^3 = 2$. Prowadzi to bezpośrednio do sprzeczności. Istnieje bowiem tylko jedna liczba rzeczywista będąca pierwiastkiem trzeciego stopnia z liczby 2, pozostałe pierwiastki są zespolone; pierwiastek $x - y\sqrt{a}$ jest, oczywiście, liczbą rzeczywistą, ponieważ liczby $x, y, \sqrt{a}$ są rzeczywiste. Zatem $\sqrt[3]{2}$ nie jest liczbą konstruowalną.

Udowodniliśmy powyżej, że liczba $\sqrt[3]{2}$ jest niekonstruowalna, skąd wnioskujemy o nierozwiązalności podwojenia sześcianu za pomocą cyrkla i linijki.

ZADANIA

Zad.2.1 (a) Uzasadnij, że $\sqrt{3/5}$ nie jest liczbą wymierną, oraz że zbiór liczb postaci $a + b\sqrt{3/5}$ gdzie a i b są wymierne, jest ciałem.

(b) Dla liczb $p = (2/3) + \sqrt{3/5}$ oraz $q = 1 - (1/2)\sqrt{3/5}$ przedstaw ich sumę, różnię, iloczyn i iloraz w postaci $a + b\sqrt{3/5}$ gdzie $a, b \in Q$.

Zad.2.2 Uzasadnij, że pierwiastki kwadratowe z liczb $5, \frac{2}{3}, 2 + \sqrt{3}$ oraz $\sqrt{3}$ nie należą do ciała $Q(\sqrt{3})$.

Zad.2.3 Oznaczmy przez F ciało $Q(\sqrt{3})$, zaś przez k liczbę $2 + \sqrt{3}$.

(a) Niech $p = 1 - \sqrt{3} - (1 + 2\sqrt{3})\sqrt{k}$ i $q = 2 + \sqrt{3} + (1 + \sqrt{3})\sqrt{k}$ będą liczbami z rozszerzenia kwadratowego $F(\sqrt{k})$. Przedstaw sumę, różnicę, iloczyn i iloraz liczb p i q w postaci $a + b\sqrt{k}$, gdzie a i b są liczbami z ciała F.

(b) Czy liczba $\sqrt{3} + \sqrt{6 + 3\sqrt{3}}$ należy do ciała $F(\sqrt{k})$?

Zad.2.4 Niech $F_1 = Q(\sqrt{3})$ i $F_2 = F_1(\sqrt{2 + \sqrt{3}})$ będą rozszerzeniami kwadratowymi. Znajdź postać ogólną elementów z ciała F_2. Zrób to samo dla $F_1 = Q(\sqrt{3})$ i $F_2 = F_1(\sqrt{\sqrt{3}})$.

Zad.2.5 Niech F będzie ciałem liczb postaci $p + q\sqrt[4]{2}$, gdzie p i q wyrażają się jako $a + b\sqrt{2}$ dla a i b wymiernych. Przedstaw w tej postaci liczbę $\frac{1}{\sqrt{2} + \sqrt[4]{2} + \sqrt{2}\sqrt[4]{2}}$ należącą do tego ciała.

Zad.2.6 Znajdź ciągi rozszerzeń kwadratowych dla następujących liczb konstruowalnych:

$$\frac{1}{\sqrt{2\sqrt{3} + 1}}, \frac{\sqrt{2} + \sqrt{3}}{1 + \sqrt{6}}, \sqrt{2} - \sqrt{2 - \sqrt{2}}, 2 - \sqrt{3} + \sqrt[4]{3}.$$

Zad.2.7 (a) Uzasadnij, że zbiór ***K*** wszystkich liczb konstruowalnych jest ciałem.

(b) Uzasadnij, że ciało ***K*** liczb konstruowalnych nie posiada żadnego rozszerzenia kwadratowego.

Zad.2.8 Uzasadnij, że $\sqrt[3]{2}$ jest liczbą niewymierną. A jak będzie z pierwiastkami wyższych stopni.

Zad.2.9 Udowodnij twierdzenie greckiego matematyka Teajteta z IV w. p.n.e. mówiące, że dla n naturalnych liczba $\sqrt{n}$ jest wymierna tylko wtedy gdy n jest kwadratem liczby naturalnej. A jak będzie z pierwiastkami wyższych stopni?

Zad.2.10 Zastosuj rozumowanie poznane na wykładzie do uzasadnienia, że konstrukcja potrojenia sześcianu jest niewykonalna. Dla jakich n naturalnych konstrukcja n-krotnego powiększenia sześcianu jest wykonalna, a dla jakich nie?

Zad.2.11 Rozstrzygnij dla jakich naturalnych n_1, n_2, n_3 wykonalna jest konstrukcja sześcianu o objętości równej objętości prostopadłościanu o krawędziach n_1, n_2, n_3.

Zad.2.12 Zbadaj, czy zawsze wykonalna jest przy pomocy cyrkla i linijki konstrukcja odcinka, którego długość równa jest średniej a. arytmetycznej, b. geometrycznej, c. harmonicznej, d. kwadratowej z długości a, b, c danych trzech odcinków.

Zad.2.13 Dany jest odcinek a oraz dwa razy dłuższy odcinek d. Czy można za pomocą cyrkla i linijki skonstruować takie odcinki b i c, że długości a, b, c, d tworzą ciąg geometryczny?

ROZDZIAŁ III

Pierwiastki wielomianów stopnia 3. Niekonstruowalność.

Fakt, że $\sqrt[3]{2}$ jest liczbą niekonstruowalną można uogólnić na inne pierwiastki równań stopnia 3.

Twierdzenie 3.1

Jeśli wielomian $a_3x^3 + a_2x^2 + a_1x + a_0$ o wymiernych współczynnikach nie ma wymiernych pierwiastków, to każdy jego (rzeczywisty) pierwiastek jest liczbą niekonstruowalną.

Zauważmy, że założenie o posiadaniu przez wielomian pierwiastków wymiernych jest kluczowe. Jeśli wielomian ma wymierny pierwiastek *a*, to możemy go przedstawić w postaci $W(x) = P(x) \cdot (x - a)$, gdzie $P(x)$ jest trójmianem kwadratowym o wymiernych współczynnikach. Z rozdziału pierwszego wiemy, że jeżeli taki trójmian ma pierwiastki, to są one konstruowalne. Czyli gdy jeden z pierwiastków wielomianu stopnia 3 jest wymierny, to pozostałe pierwiastki (o ile istnieją) są konstruowalne.

Zanim przejdziemy do dowodu twierdzenia 3.1 uzasadnijmy prawdziwość pomocniczych lematów.

Lemat 3.2 (wzór Viete'a)

Jeśli p_1, p_2, p_3 są różnymi pierwiastkami wielomianu $W(x) = a_3x^3 + a_2x^2 + a_1x + a_0$,

to $p_1 + p_2 + p_3 = -\frac{a_2}{a_3}$.

Dowód

Jeśli p_1, p_2, p_3 są różnymi pierwiastkami $W(x)$, to zachodzą poniższe równości

$$a_3x^3 + a_2x^2 + a_1x + a_0 = a_3(x - p_1)(x - p_2)(x - p_{31}) =$$

$$= a_3x^3 - a_3(p_1 + p_2 + p_3)x^2 + a_3(p_1p_2 + p_1p_3 + p_2p_3)x - a_3p_1p_2p_3$$

Porównując współczynniki przy x^2 otrzymujemy $a_2 = -a_3(p_1 + p_2 + p_3)$, stąd $p_1 + p_2 + p_3 = -\frac{a_2}{a_3}$.

Lemat 3.3

Jeżeli wielomian $W(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ ma dwa różne pierwiastki, to liczba wyznaczona przez wzór Viete'a też jest pierwiastkiem tego wielomianu.

Dowód

Skoro $W(x)$ ma pierwiastki p_1, p_2, to dzieli się on przez iloczyn $(x - p_1)(x - p_2)$. Wówczas wielomian W ma postać $W(x) = (x - p_1)(x - p_{21})(ax + b_1)$. Zatem pierwiastek $\frac{-b}{a}$ wielomianu $ax + b$ jest trzecim pierwiastkiem wielomianu $W(x)$. Z lematu 3.2 ten trzeci pierwiastek spełnia wzór Viete'y, więc można go było wyznaczyć z tego wzoru.

Teraz możemy przystąpić do dowodu zasadniczego twierdzenia.

Dowód twierdzenia 3.1

Załóżmy, że przynajmniej jeden pierwiastek jest konstruowalny. Dla każdego konstruowalnego pierwiastka rozważmy najkrótszy możliwy ciąg rozszerzeń kwadratowych $Q = F_0 \subset F_1 \subset \ldots \subset F_k$, gdzie p należy do F_k. Rozważmy ten z konstruowalnych pierwiastków, którego powyższy ciąg jest najkrótszy. Wtedy p należy do F_k oraz żaden z pierwiastków nie należy do F_{k-1}. Załóżmy, że $F_k = F_{k-1}(\sqrt{w})$, gdzie w należy do F_{k-1}. Wtedy p jest postaci $x + y\sqrt{w}$, gdzie x, y należą do F_{k-1}. Liczba p jest pierwiastkiem wielomianu, więc spełnia równanie

$$a_3(x + y\sqrt{w})^3 + a_2(x + y\sqrt{w})^2 + a_1(x + y\sqrt{w}) + a_0 = 0.$$

Obliczając, otrzymujemy równanie w postaci

$$(a_3x^3 + 3a_3xy^2w + a_2x^2 + a_2y^2w + a_1x + a_0) + (3a_3x^2y + 2a_2xy + a_1y)\sqrt{w} = 0.$$

Wyrażenia w nawiasach zastąpmy odpowiednio przez A i B, otrzymujemy wtedy równość $A + B\sqrt{w} = 0$. Zatem $A = B = 0$. Sprawdźmy teraz, że liczba $p' = x - y\sqrt{w}$ też jest pierwiastkiem wielomianu. W tym celu obliczmy wartość wielomianu dla p', mamy więc $a_3\left(x - y\sqrt{w}\right)^3 + a_2\left(x - y\sqrt{w}\right)^2 + a_1\left(x - y\sqrt{w}\right) + a_0 = A - B\sqrt{w} = 0$ (ponieważ wyliczyliśmy już, że $A = B = 0$). Zatem p' jest różnym od p pierwiastkiem wielomian.

Na mocy lematu 3.3 możemy wyznaczyć trzeci pierwiastek p_3 ze wzoru Viete'y, czyli $p + p' + p_3 = -\frac{a_2}{a_3}$. Wyliczając p_3 otrzymujemy

$$p_3 = -\frac{a_2}{a_3} - (p + p') = -\frac{a_2}{a_3} - \left(x + y\sqrt{w} + x - y\sqrt{w}\right) = -\frac{a_2}{a_3} - 2x.$$

Wtedy p_3 jest elementem F_{k-1} (bo a_2, a_3, x należą do F_{k-1}), co jest sprzeczne z wcześniejszym założeniem. Zatem każdy pierwiastek jest liczbą niekonstruowalną.

Zauważmy, że z powyższego twierdzenia wynika także niekonstruowalność liczby $\sqrt[3]{2}$. Ponieważ wielomian $x^3 - 2$, którego jedynym rzeczywistym pierwiastkiem jest $\sqrt[3]{2}$, nie ma pierwiastków wymiernych.

W rozstrzyganiu czy dany wielomian o współczynnikach całkowitych posiada wymierne pierwiastki przydatny będzie następujący lemat.

Lemat 3.4

Jeśli wielomian $W(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ o całkowitych współczynnikach ma pierwiastek wymierny wyrażony w postaci nieskracalnej jako $\frac{p}{q}$, to p dzieli a_0 i q dzieli a_n.

Dowód

$\frac{p}{q}$ jest pierwiastkiem wielomianu $W(x)$, więc zachodzi równość $a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$. Mnożąc obustronnie przez q^n otrzymujemy $a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n = 0$, co możemy zapisać równoważnie jako

$a_n p^n = q\left(a_{n-1}p^{n-1} + \ldots + a_1 pq^{n-2} + a_0 q^{n-1}\right)$. Prawa strona równości jest podzielna przez q, więc lewa też dzieli się przez q. Ponieważ p i q są względnie pierwsze, to q dzieli a_n.
Podobnie otrzymujemy $a_0 q^n = -p\left(a_n p^{n-1} + a_{n-1}p^{n-2}q + \ldots + a_1 q^{n-1}\right)$. Stosując rozumowanie jak wyżej stwierdzamy, że a_0 dzieli się przez p.

Zobaczmy jak działa nasze kryterium na przykładzie.

Przykład 3.5

Mamy wielomian $W(x) = 8x^3 - 6x - 1$. Na podstawie lematu 3.4, jeśli $\frac{p}{q}$ jest pierwiastkiem, to $p|1$ i $q|8$, czyli $p \in \{-1,1\}$, $q \in \{-1,1,-2,2,-4,4,-8,8\}$, więc $\frac{p}{q} \in \left\{-1,1,-\frac{1}{2},\frac{1}{2},-\frac{1}{4},\frac{1}{4},-\frac{1}{8},\frac{1}{8}\right\}$.
Sprawdźmy, czy któraś z potencjalnych liczb wymiernych jest pierwiastkiem. W tym celu obliczmy wartości $W(x)$ dla każdej z tych liczb:

$W(1) = 8 - 6 - 1 = 1 \neq 0$

$W(-1) = -8 + 6 - 1 = -3 \neq 0$

$W\left(\frac{1}{2}\right) = 8 \cdot \frac{1}{8} - 6 \cdot \frac{1}{2} - 1 = -3 \neq 0$

$W\left(-\frac{1}{2}\right) = -8 \cdot \frac{1}{8} + 6 \cdot \frac{1}{2} - 1 = 1 \neq 0$

$W\left(\frac{1}{4}\right) = 8 \cdot \frac{1}{64} - 6 \cdot \frac{1}{4} - 1 = -2\frac{3}{8} \neq 0$

$W\left(-\frac{1}{4}\right) = -8 \cdot \frac{1}{64} + 6 \cdot \frac{1}{4} - 1 = \frac{3}{8} \neq 0$

$W\left(\frac{1}{8}\right) = 8 \cdot \frac{1}{512} - 6 \cdot \frac{1}{8} - 1 = -1\frac{47}{64} \neq 0$

$W\left(-\frac{1}{8}\right) = -8 \cdot \frac{1}{512} + 6 \cdot \frac{1}{8} - 1 = -\frac{17}{64} \neq 0$

Żadna liczba ze zbioru $\left\{-1,1,-\frac{1}{2},\frac{1}{2},-\frac{1}{4},\frac{1}{4},-\frac{1}{8},\frac{1}{8}\right\}$ nie jest pierwiastkiem wielomianu. Zatem $W(x)$ nie ma wymiernych pierwiastków.

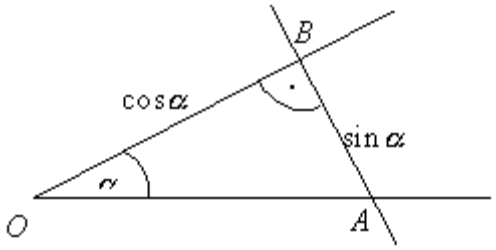
Teraz jesteśmy należycie przygotowani do rozważenia starożytnych zagadnień trysekcji kąta i zbudowania siedmiokąta foremnego.

Przykład 3.6

Udowodnimy najpierw, że trysekcja kąta za pomocą samego cyrkla i linijki jest na ogół niemożliwa. Są oczywiście kąty jak np. 90º i 180º, dla których można przeprowadzić trysekcję. Mamy natomiast wykazać, że nie można dokonać trysekcji za pomocą postępowania, które dałoby się zastosować do każdego kąta. Dla dowodu wystarczy podać jeden tylko kąt, który nie da się podzielić na trzy równe części, ponieważ ogólna metoda konstrukcji powinna stosować się do każdego poszczególnego przypadku. Wobec tego udowodnimy, że trysekcja kąta 60º jest niewykonalna. Nasze zadanie sprowadza się pokazania, że nie da się skonstruować kąta 20º.

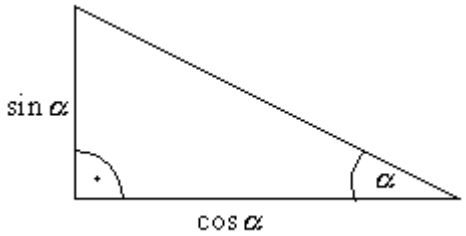
Zauważmy, że konstruowalność dowolnego kąta α zależy od tego, czy liczba $\cos\alpha$ (lub $\sin\alpha$, lub $tg\alpha$) jest konstruowalna.

Mając dany kąt α możemy skonstruować liczby $\cos\alpha$ i $\sin\alpha$. Konstrukcja ta przebiega w następujący sposób (rys.1).



Rysunek 1

Na jednym ramieniu kąta α odkładamy odcinek jednostkowy o końcach w wierzchołku *O* i punkcie *A*. Prowadzimy prostą prostopadła do drugiego ramienia kąta i przechodzącą przez punkt *A*. Otrzymaliśmy trójkąt prostokątny *OAB*, w którym długości przyprostokątnych są odpowiednio równe liczbom $\cos\alpha$ i $\sin\alpha$.



Rysunek 2

Mając dany odcinek długości $\cos\alpha$ potrafimy skonstruować odcinek $\sin\alpha$ (ponieważ $\sin\alpha = \sqrt{1-\cos^2\alpha}$). Konstruując trójkąt prostokątny jak na rysunku 2 otrzymujemy również konstrukcję kąta α.

Podobnie pokazuje się równoważność konstrukcji kąta α konstruowalności liczby $\sin\alpha$ lub $tg\alpha$.

Zatem w naszym przypadku musimy pokazać, że liczba cos20º nie należy do **K**. Na podstawie prostego wzoru trygonometrycznego $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ otrzymujemy związek pomiędzy cosinusami kątów α i 3α. Zastosujemy ten wzór do $\alpha = 20°$. Otrzymujemy, że $\cos 60° = 4\cos^3 20° - 3\cos 20°$. Podstawiając $x = \cos 20°$ i wartość $\cos 60° = \frac{1}{2}$ otrzymujemy równanie trzeciego stopnia postaci: $8x^3 - 6x - 1 = 0$.

Na mocy twierdzenia 3.1 wystarczy tylko udowodnić, że równanie to nie ma pierwiastka wymiernego. Fakt ten pokazaliśmy w przykładzie 3.5. Zatem każde rozwiązanie tego równania jest liczbą niekonstruowalną, w szczególności $\cos\alpha$, więc i kąt 20º, jest niekonstruowalny. Zadanie trysekcji dowolnego kąta jest więc niewykonalne.

Z powyższego przykładu możemy wywnioskować, że konstrukcja kąta 40º również jest niewykonalna. Gdyby dało się skonstruować kąt 40º, to prowadząc dwusieczną mielibyśmy konstrukcję kąta 20º, a wiemy, że kąt 20º jest niekonstruowalny. Idąc dalej możemy stwierdzić, że nie da się skonstruować 9-kąta foremnego (ponieważ 360º:9=40º).

Zastanówmy się teraz nad możliwością zbudowania 7-kąta foremnego.

Przykład 3.7

Rozważmy zagadnienie wyznaczenia boku 7-kąta foremnego wpisanego w koło jednostkowe. Najprostszy sposób podejścia do tego zagadnienia polega na zastosowaniu liczb zespolonych. Na płaszczyźnie zespolonej wierzchołki 7-kąta foremnego opisują się jako pierwiastki równania

(1) $$z^7 - 1 = 0.$$

Wiemy, że pierwiastek siódmego stopnia z jedności dany jest wzorem $z = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$, gdzie kąt $\frac{2\pi}{7}$ jest kątem środkowym opartym na boku 7-kąta. Zatem konstrukcja 7-kąta foremnego jest równoważna konstrukcji kąta $\frac{2\pi}{7}$, czyli liczby $\cos\frac{2\pi}{7}$. Wiemy również, że $\bar{z} = \frac{1}{z}$, a więc $a = z + \frac{1}{z} = 2\cos\frac{2\pi}{7}$. Konstrukcja siedmiokąta sprowadza się do konstrukcji liczby *a*.

Jednym z pierwiastków (1) jest $z = 1$, a pozostałe są pierwiastkami równania

(2) $$\frac{z^7-1}{z-1}=z^6+z^5+z^4+z^3+z^2+z^1+1=0,$$

które otrzymujemy z równania (1) dzieląc przez czynnik $z-1$.

Dzieląc równanie (2) przez z^3 otrzymujemy równanie

(3) $$z^3+\frac{1}{z^3}+z^2+\frac{1}{z^2}+z+\frac{1}{z}+1=0$$

Stosując proste przekształcenia algebraiczne możemy zapisać równanie (3) w postaci

(4) $$\left(z+\frac{1}{z}\right)^3-3\left(z+\frac{1}{z}\right)+\left(z+\frac{1}{z}\right)^2-2+\left(z+\frac{1}{z}\right)+1=0$$

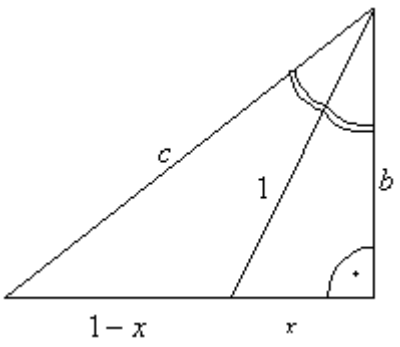
Podstawiając do (4) $a=z+\frac{1}{z}$ otrzymujemy $a^3+a^2-2a-1=0$.

Czyli a jest pierwiastkiem wielomianu $W(x)=x^3+x^2-2x-1$. Wystarczy zatem rozstrzygnąć, czy wielomian $W(x)$ ma pierwiastki wymierne. Z lematu 3.4 wiemy, że jedynymi możliwymi pierwiastkami wymiernymi są liczby –1 i 1. Obliczając $W(-1)=1$ i $W(1)=-1$ stwierdzamy, że wielomian $W(x)$ nie ma pierwiastków wymiernych i na mocy twierdzenia 3.1 każdy jego pierwiastek jest niekonstruowalny. Jeżeli liczba $a=2\cos\frac{2\pi}{7}$ jest niekonstruowalna, to $\cos\frac{2\pi}{7}$ też, a więc możemy stwierdzić, że nie istnieje konstrukcja 7-kąta foremnego.

Na koniec rozstrzygnijmy wykonalność poniższej konstrukcji.

Przykład 3.8

Sprawdźmy konstruowalność trójkąta prostokątnego, którego jedna przyprostokątna i dwusieczna opuszczona na tą przyprostokątną mają długość 1 (rys.3).



Rysunek 3

Zauważmy, że do konstrukcji tego trójkąta wystarczy skonstruować drugą przyprostokątną *b*. Niech dwusieczna dzieli przyprostokątną długości 1 w stosunku $\frac{x}{1-x}$. Stosując twierdzenie Pitagorasa otrzymujemy długość *x* równą $\sqrt{1-b^2}$ oraz długość przeciwprostokątnej *c* równą $\sqrt{1+b^2}$. Z własności dwusiecznej wiemy, że prawdziwa jest następująca równość $\frac{x}{1-x}=\frac{b}{c}$. Podstawiając za *x* i *c* wyliczone wcześniej wartości dostajemy równanie $\frac{\sqrt{1-b^2}}{1-\sqrt{1-b^2}}=\frac{b}{\sqrt{1+b^2}}$. Wykonując kolejne przekształcenia ostatecznie otrzymujemy równanie postaci $4b^6-4b^2+1=0$. Podstawmy do równania $a=b^2$, stąd mamy postać $4a^3-4a+1=0$. Konstruowalność liczby *b* jest równoważna konstruowalności liczby *a*. Zbadajmy zatem czy wielomian $4x^3-4x+1$, którego *a* jest pierwiastkiem, ma pierwiastki wymierne. Z lematu 3.4 wiemy, że jedynymi możliwymi pierwiastkami wymiernymi są liczby ze zbioru $\{-1,1,-\frac{1}{2},\frac{1}{2},-\frac{1}{4},\frac{1}{4}\}$. Obliczając wartości wielomianu dla każdej z tych liczb stwierdzamy, że wielomian nie ma pierwiastków wymiernych. Zatem na mocy twierdzenia 3.1 każdy jego pierwiastek jest niekonstruowalny (w szczególności *a*). Z niekonstruowalności liczby *a* wynika niekonstruowalność liczby *b*, więc również nie istnieje konstrukcja trójkąta prostokątnego spełniającego warunki zadania.

ZADANIA

Zad.3.1 Zbadaj, czy następujące wielomiany mają pierwiastki wymierne:

(a) $x^2 - 4x - 1$;

(b) $x^3 - x^2 - 13x - 3$;

(c) $4x^3 - 4x + 1$;

(d) $8x^4 - 4x^3 - 8x^2 - 2x - 1$.

A czy maja pierwiastki konstruowalne?

Zad.3.2 Czy mając dany odcinek jednostkowy można skonstruować sześcian, dla którego suma pola powierzchni i objętości wynosi: (a) 5; (b) 3? Jeśli tak, to czy można skonstruować wszystkie sześciany o tej własności?

Zad.3.3 Czy odcinek długości 4 można konstrukcyjnie podzielić na trzy odcinki, z których dwa będą jednakowe, i to w taki sposób by prostopadłościan zbudowany na tych odcinkach miał objętość równą 1?

Zad.3.4 Czy jest konstruowalny trójkąt równoramienny, którego ramię ma długość 5, a promień koła wpisanego w ten trójkąt – długość 1? Rozwiąż to zadanie następującymi etapami:

(a) Oznacz przez *d* połowę podstawy tego trójkąta i uzasadnij, że dla skonstruowania tego trójkąta potrzeba i wystarcza skonstruować odcinek *d*.

(b) Dla znalezienia wielomianu, którego pierwiastkiem jest *d* przyrównaj do siebie wyrażenia na kwadrat pola trójkąta uzyskane ze wzorów $P = pr$ oraz

$P = \sqrt{p(p-a)(p-b)(p-c)}$, gdzie p jest połową obwodu trójkąta, a, b, c są długościami jego boków, zaś r jest promieniem okręgu wpisanego.

(c) Znajdź wymierny pierwiastek q uzyskanego wielomianu czwartego stopnia, przekonaj się, że nie jest on równy d, podziel wielomian przez $x-q$ i zbadaj nowy wielomian stopnia 3.

Zad.3.5 Czy jest konstruowalny trójkąt równoramienny, którego dwusieczne mają długości 1, 1 i 2? Rozwiąż to zadanie w następujących krokach:

(a) Oznacz przez α połowę kąta przy podstawie tego trójkąta i uzasadnij, że do skonstruowania trójkąta potrzeba i wystarcza skonstruować odcinek długości $\sin\alpha$.

(b) Wyraź długość podstawy AB trójkąta w terminach kąta α przy pomocy funkcji tangens zastosowanej do trójkąta prostokątnego powstałego z rozcięcia naszego trójkąta dwusieczną spuszczoną z wierzchołka przeciwległego do podstawy.

(c) Wyraź długość podstawy AB inaczej, korzystając z twierdzenia sinusów zastosowanego do boków AB i AD trójkąta ABD, gdzie D jest drugim końcem dwusiecznej spuszczonej z wierzchołka A.

(d) Przyrównaj do siebie wyrażenia na AB otrzymane w punktach b. i c. Wszystkie występujące funkcje trygonometryczne wyraź w terminach $\sin\alpha$. Doprowadź zależność do takiej postaci, w której $\sin\alpha$ okazuje się być pierwiastkiem pewnego wielomianu trzeciego stopnia.

(e) Zbadaj otrzymany wielomian.

Zad.3.6 Czy jest wykonalny za pomocą cyrkla i linijki podział dowolnego kąta na 4, 5, 6, 7, 8, 9 równych części ?

Zad.3.7 Czy można skonstruować cyrklem i linijką kąty $5°, 10°, 15°, 25°, 40°, 75°, 85°$?

Zad.3.8 Uzasadnij metodą nie wprost, że jeśli x jest liczbą niekonstruowalna, to również niekonstruowalne są następujące liczby: $\frac{1}{2}x, \sqrt{x}, \sqrt{x+1}, x^2, x^2+2, x^2+3x+1$. Czy liczba x^3 też musi być liczbą niekonstruowalną?

ROZDZIAŁ IV

Liczby algebraiczne.

Nasze dalsze rozważania mają na celu dostarczenie nam nowych argumentów w rozstrzyganiu konstruowalności liczb. Wraz z rozwojem teorii uzasadnimy między innymi twierdzenie 4.1.

Twierdzenie 4.1

Jeśli wielomian *W(x)* o współczynnikach wymiernych jest nierozkładalny nad ***Q***, to znaczy nie da się przedstawić jako iloczyn *W(x)=P(x)Q(x)* wielomianów o współczynnikach wymiernych stopni większych lub równych 1, i jeśli stopień *W(x)* nie jest potęgą liczby 2, to wszystkie pierwiastki wielomianu *W(x)* są niekonstruowalne.

Ta wiedza przyda nam się też w rozdziale VI do rozstrzygania konstruowalności wielokątów foremnych.

Zauważmy, że w przypadku wielomianów stopnia 3 nierozkładalność nad ***Q*** jest tym samym co nieposiadanie wymiernego pierwiastka. Ponieważ rozkład wielomianu stopnia 3 musi mieć postać $W(x)=(ax^2+bx+c)(dx+e)$, gdzie *a, b, c, d, e* są wymierne. Jest to równoważne temu, że liczba $\frac{-e}{d}$ jest wymiernym pierwiastkiem *W(x)*. Dla wielomianów

wyższych stopni własność ta nie zachodzi. Istnieją bowiem wielomiany, które nie posiadają wymiernego pierwiastka a pomimo to są rozkładalne (np. wielomian piątego stopnia może się rozłożyć na iloczyn wielomianów stopni dwa i trzy, z którego żaden nie posiada wymiernego pierwiastka). W twierdzeniu 4.1 istotne jest założenie o stopniu wielomianu. Dla wielomianów stopnia 2^k łatwo możemy podać kontrprzykłady na to twierdzenie (np. wielomian x^4-2 jest nierozkładalny nad $\boldsymbol{Q}$, ale jego pierwiastek $\sqrt[4]{2}=\sqrt{\sqrt{2}}$ jest konstruowalny).

Zacznijmy od zdefiniowania liczb algebraicznych.

Definicja 4.2

Liczbą algebraiczną nazywamy liczbę *u*, która jest pierwiastkiem wielomianu $W(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1 x+a_0$ dowolnego stopnia *n* o wymiernych współczynnikach.

Zauważmy , że równie dobrze liczba algebraiczna *u* jest pierwiastkiem wielomianu o współczynnikach całkowitych. Na przykład jeśli *u* spełnia równanie $\frac{3}{7}u^3+1\frac{1}{4}u^2-\frac{9}{14}=0$, to mnożąc obustronnie przez 28 dostaniemy równanie $12u^3+35u^2-18=0$.

Dla stwierdzenia, że współczynniki wielomianu W są wymierne wprowadźmy oznaczenie: $W(x)\in Q[x]$.

Dowolny wielomian z $Q[x]$, którego pierwiastkiem jest *u* będziemy też nazywać wielomianem zerującym *u*.

Przyjrzyjmy się teraz przykładom liczb algebraicznych.

Przykład 4.3

- Liczby wymierne *q* są algebraiczne jako pierwiastki wielomianów $W(x)=x-q$, $W(x)\in Q[x]$.
- Pierwiastki $\sqrt[n]{q}$ z liczb wymiernych *q* spełniają równanie $x^n-q=0$, więc są algebraiczne.
- Uzasadnijmy, że liczba $a=\sqrt{2}+1$ jest algebraiczna. W tym celu poszukajmy wielomianu $W(x)\in Q[x]$, którego *a* jest pierwiastkiem. Równość $a=\sqrt{2}+1$ możemy zapisać równoważnie jako $a-1=\sqrt{2}$, podnosząc obustronnie do kwadratu i

porządkując otrzymujemy równanie $a^2 - 2a - 1 = 0$. Zatem liczba *a* jest pierwiastkiem $W(x) = x^2 - 2x - 1$, czyli *a* jest algebraiczna.

Wielomian minimalny liczby algebraicznej.

Zauważmy, że dana liczba algebraiczna *u* jest pierwiastkiem wielu różnych wielomianów z $Q[x]$. Na przykład liczba $\sqrt[3]{2}$ jest pierwiastkiem wielomianu $W(x) = x^3 - 2$, ale jest także pierwiastkiem wielomianów $W_1(x) = 2x^3 - 4$, $W_2(x) = \frac{1}{3}x^3 - \frac{2}{3}$, $W_3(x) = (x^3 - 2)(x + 1) = x^4 + x^3 - 2x - 2$, itd. Zauważmy , że mnożąc $x^3 - 2$ przez dowolny wielomian z $Q[x]$ możemy otrzymać wielomian z $Q[x]$ dowolnie dużego stopnia, którego pierwiastkiem jest $\sqrt[3]{2}$. Czyli $\sqrt[3]{2}$ jest pierwiastkiem wielomianu z $Q[x]$ dowolnie dużego stopnia większego od 2.

Wprowadźmy zatem definicję.

Definicja 4.4

Wielomianem minimalnym liczby algebraicznej *u* nazywamy dowolny wielomian z $Q[x]$ zerujący *u* najmniejszego stopnia wśród wielomianów zerujących *u*.

Dla wielomianów minimalnych zachodzą poniższe twierdzenia.

Twierdzenie 4.5

Wielomian minimalny liczby algebraicznej *u* jest jednoznacznie wyznaczony z dokładnością do mnożenia przez liczbę wymierną .

Dowód

Załóżmy, że istnieją dwa wielomiany minimalne liczby *u*: $P(x) = a_n x^n + \ldots + a_0$ i $Q(x) = b_n x^n + \ldots + b_0$ (nie takie, że jeden jest iloczynem drugiego przez liczbę wymierną).

Mnożąc $Q(x)$ przez $\frac{a_n}{b_n}$ otrzymujemy wielomian minimalny

$$Q'(x) = a_n x^n + \frac{a_n}{b_n} b_{n-1} x^{n-1} + \ldots + \frac{a_n}{b_n} b_0 .$$

Współczynniki przy najwyższej potędze w wielomianach $P(x)$ i $Q'(x)$ są równe, więc odejmując je od siebie otrzymamy niezerowy wielomian niższego stopnia $S(x) = P(x) - Q'(x)$. Zauważmy, że liczba *u* też jest pierwiastkiem $S(x)$, ponieważ $P(u) = Q(u) = 0$, skąd $S(u) = P(u) - Q'(u) = P(u) - \frac{a_n}{b_n} Q(u) = 0$. Czyli znaleźliśmy wielomian niższego stopnia niż $P(x)$ i $Q(x)$, którego pierwiastkiem jest liczba *u*. Daje to sprzeczność z założeniem, że $P(x)$ i $Q(x)$ są minimalne. Zatem wielomian minimalny jest jednoznaczny z dokładnością do mnożenia przez liczbę wymierną.

Twierdzenie 4.6

Wielomian minimalny $W(x)$ liczby algebraicznej *u* jest nierozkładalny nad $\boldsymbol{Q}$.

Dowód

Załóżmy, że $W(x)$ jest rozkładalny. Możemy więc przedstawić go w postaci iloczynu wielomianów niższego stopnia $P_1(x)$, $P_2(x) \in Q[x]$, czyli $W(x) = P_1(x) \cdot P_2(x)$. Ponieważ *u* jest pierwiastkiem $W(x)$, to $W(u) = P_1(u) \cdot P_2(u) = 0$. Zatem zachodzi jedna z następujących równości $P_1(u) = 0$ lub $P_2(u) = 0$. Otrzymaliśmy więc wielomian niższego stopnia niż $W(x)$, którego u jest pierwiastkiem. Co jest sprzeczne z minimalnością wielomianu $W(x)$. Stąd wielomian $W(x)$ jest nierozkładalny.

Twierdzenie 4.7

Dla danej liczby algebraicznej *u*, każdy wielomian $V(x) \in Q[x]$ mający *u* jako pierwiastek jest podzielny przez wielomian minimalny $W(x)$ liczby *u*.

Dowód

Podzielmy $V(x)$ przez $W(x)$, otrzymując być może resztę, czyli $V(x) = W(x) \cdot P(x) + R(x)$. Wiemy, że $P(x)$ i $R(x) \in Q[x]$ oraz, że stopień $R(x)$ jest niższy od stopnia $W(x)$. Gdyby reszta $R(x)$ nie była wielomianem zerowym, to byłaby wielomianem

niższego stopnia niż $W(x)$ mającym *u* za pierwiastek, ponieważ $V(u) = W(u) = 0$ więc również $R(u) = V(u) - W(u) \cdot P(u) = 0$. Zatem $R(x)$ jest wielomianem zerowym, co oznacza, że $V(x)$ dzieli się przez $W(x)$.

Twierdzenie 4.8

Wielomian $W(x) \in Q[x]$ nierozkładalny nad $\boldsymbol{Q}$ jest wielomianem minimalnym dla wszystkich swoich pierwiastków.

Dowód

Załóżmy, że $W(x)$ nie jest wielomianem minimalnym dla pewnego swojego pierwiastka *u*. Niech więc $Z(x)$ będzie wielomianem minimalnym tego pierwiastka. Wtedy, na mocy twierdzenia 4.7, $W(x)$ dzieli się przez $Z(x)$, czyli $W(x) = Z(x) \cdot P(x)$, gdzie $P(x) \in Q[x]$. Otrzymaliśmy rozkład wielomianu $W(x)$ wbrew twierdzeniu 4.6. Zatem $W(x)$ jest minimalny dla każdego pierwiastka.

Z pojęciem wielomianu minimalnego wiąże się poniższa definicja.

Definicja 4.9

Stopniem liczby algebraicznej *u* nazywamy stopień jej wielomianu minimalnego.

Przyjrzyjmy się niektórym przykładom liczb algebraicznych stopnia 1, 2 i 3.

Przykład 4.10

- Liczby wymierne, jako jedyne, są liczbami algebraicznymi stopnia 1.
- Niewymierne pierwiastki $\sqrt{q}$ z liczb wymiernych są liczbami algebraicznymi drugiego stopnia. Ponieważ wielomian $x^2 - q$, nierozkładalny nad $\boldsymbol{Q}$, jest wielomianem minimalnym $\sqrt{q}$. Istnieją jeszcze inne liczby stopnia 2, ich pełną charakteryzację zostawiamy jako ćwiczenie.
- Pierwiastki wielomianów stopnia 3 z $Q[x]$ nie mających pierwiastków wymiernych (czyli niekonstruowalne pierwiastki wielomianów stopnia 3) są liczbami

algebraicznymi stopnia 3, bo ich wielomianem minimalnym jest powyższy nierozkładalny nad $\boldsymbol{Q}$ wielomian stopnia 3.

Rozszerzenie ciała liczb wymiernych o liczbę algebraiczną.

W rozdziale II rozszerzaliśmy dowolne ciało liczbowe o pierwiastek kwadratowy tzw. rozszerzenie kwadratowe. Podobnie możemy rozszerzyć ciało liczb wymiernych o dowolną liczbę algebraiczną. Zdefiniujmy zatem takie rozszerzenie.

Definicja 4.11

Rozszerzeniem ciała $\boldsymbol{Q}$ o liczbę algebraiczną u nazywamy najmniejsze możliwe ciało liczbowe zawierające $\boldsymbol{Q}$ oraz liczbę u. Oznaczamy je $Q(u)$.

Dla tak zdefiniowanego rozszerzenia $Q(u)$ prawdziwe jest następujące twierdzenie.

Twierdzenie 4.12

Jeżeli u jest liczbą algebraiczną stopnia k, to ciało $Q(u)$ składa się z liczb postaci

(1) $$q_0 + q_1u + q_2u^2 + \ldots + q_{k-1}u^{k-1},$$

gdzie q_0, q_1, $\cdots$, q_{k-1} są wymierne. Ponadto, każda liczba z ciała $Q(u)$ ma jednoznaczne przedstawienie w postaci (1).

Dowód

Liczba u należy do $Q(u)$, więc także liczby postaci (1) należą do $Q(u)$. Aby przekonać się, że liczby te tworzą ciało wystarczy sprawdzić, że ich sumy, różnice, iloczyny i ilorazy też mają postać (1).

Dla sumy i różnicy dowód jest łatwy więc go pomijamy. Iloczyn pokażemy na przykładzie liczby algebraicznej u, będącej pierwiastkiem wielomianu $V(x) = x^3 - x^2 - 1$.

Dla każdego innego wielomianu możemy przeprowadzić analogiczny dowód.

Rozważmy zatem liczby $a = q_0 + q_1u + q_2u^2$ i $b = p_0 + p_1u + p_2u^2$ z ciała $Q(u)$. Wtedy iloczyn a i b jest postaci

$$ab = p_2q_2u^4 + (p_1q_2 + p_2q_1)u^3 + (p_0q_2 + p_1q_1 + p_2q_0)u^2 + (p_0q_1 + p_1q_0)u + p_0q_0 = W(u).$$

Podzielmy wielomian $W(x)$ przez $V(x)$. Stąd $W(x)=V(x)\cdot(Ax+Bx)+(Cx^2+Dx+E)$, gdzie *A, B, C, D, E* są wymierne, a wielomian Cx^2+Dx+E jest resztą z dzielenia $W(x)$ przez $V(x)$. Wykorzystując fakt, że $V(u)=0$, otrzymujemy, że $ab=W(u)=V(u)\cdot(Au+Bu)+(Cu^2+Du+E)=E+Du+Cu^2$, gdzie *E, D, C* są wymierne. Jest to szukana postać (1) iloczynu liczb *ab*.

Zamiast ilorazu wystarczy teraz rozważyć odwrotność liczby mającej postać (1). Posłużymy się tym samym przykładem liczby *u* (o wielomianie minimalnym $V(x)$). Dla liczby $\frac{1}{1+2u-3u^2}$ szukamy postaci $A+Bu+Cu^2$ takiej, że $(A+Bu+Cu^2)(1+2u-3u^2)=1$. Wyliczając iloczyn mamy $-3Cu^4+(2C-3B)u^3+(2B+C-3A)u^2+(2A+B)u+A=1$. Dzielimy wielomian $W(x)=-3Cx^4+(2C-3B)x^3+(2B+C-3A)x^2+(2A+B)x+A-1$ przez $V(x)$. Otrzymujemy postać $W(x)=V(x)\cdot(-3Cx-C-3B)+(-B-3A)x^2+(2A+B-3C)x+A-C-3B-1$. O reszcie $R(x)=(-B-3A)x^2+(2A+B-3C)x+A-C-3B-1$ wiemy, że $R(u)=0$. Wystarczy więc znaleźć takie wymierne współczynniki *A, B, C,* że spełniony jest układ $\begin{cases}-B-3A=0\\B+2A-3C=0\\A-C-3B-1=0\end{cases}$.

Rozwiązując powyższy układ równań liniowych, dostajemy $A=\frac{3}{31}$, $B=-\frac{9}{31}$, $C=-\frac{1}{31}$.

Zatem liczba $\frac{1}{1+2u-3u^2}$ jest równa $\frac{3}{31}-\frac{9}{31}u-\frac{1}{31}u^2$ i jest to szukana postać (1). W analogiczny sposób możemy doprowadzić do postaci (1) odwrotność każdej liczby z $Q(u)$.

Aby pokazać jednoznaczność przedstawienia w postaci (1), załóżmy nie wprost, że liczba *x* z $Q(u)$ ma dwa różne przedstawienia $x=q_0+q_1u+\ldots+q_{k-1}u^{k-1}$ i $x=p_0+p_1u+\ldots+p_{k-1}u^{k-1}$. Odejmując je stronami otrzymujemy równanie $P(u)=(p_0-q_0)+(p_1-q_1)u+\ldots+(p_{k-1}-q_{k-1})u^{k-1}=0$, którego *u* jest pierwiastkiem. Wówczas niezerowy wielomian $P(x)$ stopnia mniejszego od *k* zeruje liczbę *u*, wbrew temu, że

wielomian minimalny tej liczby ma stopień *k*. Zatem przedstawienie w postaci (1) jest jednoznaczne.

Pokazując, że zbiór $\{q_0 + q_1 u + \ldots + q_{k-1} u^{k-1} : q_0, q_1, \ldots, q_n \in Q\}$,

gdzie stopień *u* wynosi *k*, jest ciałem oraz, że każda liczba z ciała $Q(u)$ ma jednoznaczne przedstawienie w postaci (1), udowodniliśmy twierdzenie 4.12.

Zauważmy, że dzięki temu twierdzeniu nie musimy rozważać bardziej skomplikowanych postaci liczb. Ponieważ $Q(u)$ jest ciałem więc np. liczba $\frac{u^3 - 2u + 1}{u^5 - u^4 - 7}$ należy do $Q(u)$ i wobec tego daje się przedstawić w postaci wielomianowej z twierdzenia 4.12.

Baza i stopień rozszerzenia.

Do tej pory poznaliśmy rozszerzenie kwadratowe ciała *F* (czyli rozszerzenie dowolnego ciała o pierwiastek kwadratowy) oraz rozszerzenie ciała liczb wymiernych o liczbę algebraiczną . Zdefiniujmy teraz ogólnie pojęcie rozszerzenia.

Definicja 4.13

Rozszerzeniem ciała *K* nazywamy dowolne ciało *L* zawierające ciało *K*.

Rozszerzone ciało *L* będziemy traktować jako przestrzeń wektorową dla której skalarami będą elementy ciała *K*. Możemy wtedy mówić o kombinacjach liniowych $a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$, gdzie współczynniki $a_1, \ldots, a_n$ należą do *K*, a wektory $b_1, \ldots, b_n$ należą do *L*. Możemy też mówić o wymiarze *L* jako przestrzeni wektorowej z ciałem skalarów *k*. Rozszerzenie nazywamy skończonym, jeśli wspomniany wymiar *L* jest skończony. Rozszerzenia z jakimi będziemy się spotykać w tej pracy będą z reguły rozszerzeniami skończonymi.

Dla każdego skończonego rozszerzenia możemy wskazać bazę.

Definicja 4.14

Bazą skończonego rozszerzenia L ciała K nazywamy dowolny układ liczb $l_1,\ldots,l_n$ z ciała L taki, że każda liczba x należąca do L przedstawia się jednoznacznie jako kombinacja liniowa $a_1l_1+\ldots+a_nl_n$, gdzie $a_1,\ldots,a_n$ są elementami K.

Przyjrzyjmy się bazom znanych nam rozszerzeń.

Przykład 4.15

- Jako bazę rozszerzenia kwadratowego $F(\sqrt{a})$ $(a\in F,\sqrt{a}\notin F)$ ciała F można przyjąć układ liczb $1,\sqrt{a}$, ponieważ każdy element x rozszerzenia $F(\sqrt{a})$ ma postać kombinacji liniowej $x=p\cdot 1+q\cdot\sqrt{a}$, gdzie p i q należą do F. Pokażmy jeszcze, ze przedstawienie to jest jednoznaczne. Załóżmy, że liczba x ma dwa różne przedstawienia $x=p_1\cdot 1+q_1\sqrt{a}$ i $x=p_2\cdot 1+q_2\sqrt{a}$ (zachodzi przynajmniej jeden z przypadków $p_1\neq p_2,\quad q_1\neq q_2$), gdzie p_1,q_1,p_2,q_2 należą do F. Odejmując je stronami otrzymamy $p_1-p_2+(q_1-q_2)\sqrt{a}=0$. Jeżeli $q_1=q_2$ to wtedy także $p_1=p_2$, a założyliśmy, że przedstawienia liczby x są różne. Weźmy więc $q_1\neq q_2$, wówczas możemy wyznaczyć $\sqrt{a}$ z równania, czyli $\sqrt{a}=\frac{p_2-p_1}{q_1-q_2}$, ale wtedy $\sqrt{a}$ należy do F wbrew założeniu. Zatem postać $x=p\cdot 1+q\cdot\sqrt{a}$ jest jednoznaczna.
- Dla rozszerzenia o liczbę algebraiczną u stopnia k ciała liczb wymiernych jako bazę można przyjąć układ $1,u,u^2,\ldots,u^{k-1}$, ponieważ każda liczba x z $Q(u)$ ma jednoznaczną postać $x=q_0\cdot 1+q_1u+\ldots+q_{k-1}u^{k-1}$, gdzie $q_0,\ldots,q_{k-1}$ są wymierne.
  Uzasadnienie jednoznaczności tego przedstawienia było przeprowadzone w dowodzie twierdzenia 4.12, więc je pomijamy.

Zauważmy, że w powyższych przykładach rozszerzeń możemy wskazać również inne bazy (np. $1,1+\sqrt{a}$ są bazą dla $F(\sqrt{a})$). Te przyjęte przez nas są najbardziej naturalne.

Zdefiniujmy teraz pojęcie stopnia rozszerzenia.

Definicja 4.16

Stopniem rozszerzenia L ciała K nazywamy wymiar L jako przestrzeni liniowej względem ciała K lub równoważnie, liczbę elementów w dowolnej bazie rozszerzenia. Stopień ten oznaczamy symbolem $(L:K)$.

Na podstawie powyższej definicji dla rozszerzeń z przykładu 4.15 mamy $\left(F(\sqrt{a}):F\right)=2$ (dwa elementy w bazie rozszerzenia kwadratowego), $(Q(u):Q)=k$ (k elementów w bazie). Dla $Q(u)$ stopień rozszerzenia jest równy stopniowi liczby algebraicznej u. W niektórych przypadkach baza rozszerzenia ma nieskończenie wiele elementów, wtedy stopień rozszerzenia wynosi ∞, np. $(R:Q)=\infty$.

Teraz jesteśmy już przygotowani do udowodnienia następujących twierdzeń.

Twierdzenie 4.17

Jeśli M jest rozszerzeniem L, a L jest rozszerzeniem ciała K to $(M:K)=(M:L)\cdot(L:K)$.

Dowód

Załóżmy, że rozszerzenia $K\subset L$ i $L\subset M$ są skończone. Niech $(M:L)=n$, $(L:K)=k$, oraz niech $m_1,\ldots,m_n$ będą bazą rozszerzenia M, a $l_1,\ldots,l_k$ bazą rozszerzenia L. Pokażemy, że zbiór iloczynów $m_i l_j$ gdzie $i=1,\ldots,n$ $j=1,\ldots,k$, tworzy bazę rozszerzenia M ciała K. Weźmy dowolny element y ciała M. Skoro $m_1,\ldots,m_n$ jest bazą rozszerzenia M ciała L, to $y=b_1m_1+\ldots+b_nm_n$, gdzie $b_1,\ldots,b_n$ należą do L. Przedstawmy teraz każdy z współczynników b_i jako kombinację liniową bazy $l_1,\ldots,l_k$ rozszerzenia L. Czyli $b_i=a_{i1}l_1+\ldots+a_{ik}l_k$, gdzie $i=1,\ldots,n$ i $a_{i1},\ldots,a_{ik}$ należą do K.

Ostatecznie otrzymujemy postać

$$y=(a_{11}l_1+\ldots+a_{1k}l_k)m_1+\ldots+(a_{n1}l_1+\ldots+a_{nk}l_k)m_n=\sum_{\substack{i=1,\ldots,n\\ j=1,\ldots,k}}a_{ij}(m_il_j).$$

Jest to kombinacja liniowa dowolnego elementu z M. Przedstawienie to jest jednoznaczne (wynika z jednoznaczności przedstawień w bazach rozszerzeń L i K). Zatem rozszerzenie M ciała K ma bazę złożoną z nk elementów, czyli $(M:K)=(M:L)\cdot(L:K)$.

Jeżeli stopień któregoś z rozszerzeń *M, L, K* jest nieskończony to twierdzenie 4.17 dalej jest prawdziwe. Tylko wtedy w dowodzie używa się nieskończonych baz.

Twierdzenie 4.18

Jeśli *L* jest skończonym rozszerzeniem ciała $\boldsymbol{Q}$, to każda liczba *a* należąca do *L* jest liczbą algebraiczną. Ponadto stopień *a* jest dzielnikiem stopnia rozszerzenia $(L:Q)$.

Dowód

Niech $(L:Q)=n$, oraz niech *a* należy do *L*. Rozważmy układ liczb 1, $a, a^2,\ldots,a^n$ z *L*. Potraktujmy te liczby jak wektory w przestrzeni wektorowej *L* nad ciałem skalarów $\boldsymbol{Q}$. Tych wektorów jest *n+1*, czyli więcej niż wymiar *L* nad $\boldsymbol{Q}$. Zatem układ 1, $a, a^2,\ldots,a^n$ jest liniowo zależny, więc istnieją liczby wymierne $b_0, b_1,\ldots,b_n$, nie wszystkie równe zero, takie że kombinacja liniowa $b_0\cdot 1+b_1a+b_2a^2+\ldots+b_na^n$ jest równa 0. Liczba *a* jest pierwiastkiem wielomianu $W(x)=b_0+b_1a+b_2a^2+\ldots+b_na^n\in Q[x]$, czyli jest algebraiczna. Pokażmy jeszcze, że jej stopień dzieli $(L:Q)$. W tym celu rozważmy trzy ciała $Q\subset Q(a)\subset L$. Na mocy twierdzenia 4.17 mamy, że $(L:Q)=(L:Q(a))\cdot(Q(a):Q)$. Wiemy, że $(Q(a):Q)$ jest równe stopniowi liczby *a*. Ponieważ prawa strona równości dzieli się przez stopień *a*, więc $(L:Q)$ też musi dzielić się przez stopień liczby *a*.

Z powyższych twierdzeń wynika wniosek.

Wniosek 4.19

Każda liczba konstruowalna jest liczbą algebraiczną, a ponadto jej stopień jest zawsze potęgą liczby 2. Liczba algebraiczna, której stopień nie jest potęgą liczby 2, nie jest konstruowalna.

Dowód

Niech *a* będzie liczbą konstruowalną. Mamy więc dany ciąg rozszerzeń kwadratowych $Q=F_0\subset F_1\subset F_2\subset\ldots\subset F_m$, gdzie dla każdego *i* zachodzi $F_{i+1}=F_i\left(\sqrt{b_i}\right)$,

b_i należy do F_i, a jest elementem F_m. Wiemy, że $(F_{i+1} : F_i) = 2, \quad i = 0,\ldots,m$. Na mocy twierdzenia 4.17 mamy, że $(F_m : Q) = (F_m : F_{m-1}) \cdot \ldots \cdot (F_1 : Q) = 2^m$, zatem F_m jest skończonym rozszerzeniem ciała $\boldsymbol{Q}$. Ponieważ a należy do F_m, więc na podstawie twierdzenia 4.18 a jest liczbą algebraiczną, ponadto stopień a dzieli $(F_m : Q) = 2^m$. Jedynymi dzielnikami liczby 2^m są liczby postaci 2^k dla $k = 0,1,\ldots,m$, więc stopień a też jest potęgą liczby 2.

Dodatkowo z prac Carla Friedricha Gaussa i Evariste Galois wynika, że każda liczba algebraiczna stopnia 2^m jest konstruowalna. Jednak dowód tego faktu pominiemy.

Zauważmy, że druga część wniosku 4.19 dotycząca liczb algebraicznych niekonstruowalnych, jest przeformułowaniem twierdzenia 4.1 ponieważ liczba algebraiczna, której stopień nie jest potęgą liczby 2 jest pierwiastkiem wielomianu minimalnego (czyli nierozkładalnego nad *Q*) tego samego stopnia. Zatem uzasadniliśmy, wraz z wnioskiem 4.19, twierdzenie 4.1.

W teorii liczb konstruowalnych mamy więc ostateczny wyznacznik konstruowalności. Mianowicie dana liczba jest konstruowalna wtedy i tylko wtedy, gdy jest liczbą algebraiczną stopnia 2^k. Zatem niekonstruowalność liczby wynika z faktu, że jest algebraiczna stopnia różnego od 2^k, albo, że jest niealgebraiczna (przestępna). W 1874 roku Georg Cantor udowodnił następujące twierdzenie.

Twierdzenie 4.20

Istnieje przeliczalnie wiele liczb algebraicznych.

Zauważmy, że to twierdzenie świadczy o istnieniu liczb rzeczywistych nie będących liczbami algebraicznymi (ponieważ zbiór liczb $\boldsymbol{R}$ jest nieprzeliczalny).

Dowód twierdzenia 4.20

Aby pokazać, że liczb algebraicznych jest przeliczalnie wiele wystarczy pokazać, że można je ustawić w ciąg. Metoda przeliczenia zbioru liczb algebraicznych jest następująca. Każdemu równaniu postaci (2) $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$ przyporządkujemy liczbę dodatnią $h = |a_n| + |a_{n-1}| + \ldots + |a_1| + |a_0| + n$, którą nazwiemy „wysokością” równania. Dla każdej

ustalonej wartości *h* istnieje tylko skończona liczba równań postaci (2) mających wysokość *h*. Każde z tych równań może mieć co najwyżej *n* różnych pierwiastków. Zatem może być tylko skończona ilość liczb algebraicznych, których równania mają wysokość *h*, i możemy ułożyć wszystkie liczby algebraiczne w ciąg zaczynając od liczb o wysokości 1, biorąc następnie liczby wysokości 2, itd. Znaleźliśmy ciąg składający się z wszystkich liczb algebraicznych co kończy dowód twierdzenia.

Przykładami liczb niealgebraicznych są liczby π i *e*. Przestępność liczby *e* udowodnił w 1873 roku Charles Hermite, a przestępność liczby π w 1882 roku Ferdinand Lindemann. Dowody te wykraczają poza ramy naszego skryptu więc je pominiemy.

Wiedząc, że liczba π jest niealgebraiczna, czyli niekonstruowalna, możemy rozstrzygnąć problem rektyfikacji okręgu i kwadratury koła.

Przykład 4.21

Zadanie rektyfikacji czyli wyprostowania okręgu, polega na skonstruowaniu odcinka, którego długość jest równa obwodowi danego okręgu. Przyjmijmy, że dany okrąg ma promień 1. Wówczas problem sprowadza się do konstrukcji odcinka długości 2π. Gdyby 2π było konstruowalne, to $\pi = \frac{1}{2} \cdot 2\pi$ też dałoby się skonstruować, a wiemy, że π jest niekonstruowalne. Zatem zadanie rektyfikacji jest niewykonalne za pomocą cyrkla i linijki.

Przykład 4.22

Problemem kwadratury koła zajmowaliśmy się w przykładzie 1.1. Wiemy, że to zadanie sprowadza się do skonstruowania odcinka o długości $\sqrt{\pi}$, jako boku poszukiwanego kwadratu. Gdyby odcinek $\sqrt{\pi}$ był konstruowalny, to $\pi = \left(\sqrt{\pi}\right)^2$ również, a wiemy, że π jest liczbą niekonstruowalną. Zatem bok kwadratu jest niekonstruowalny, więc całe zadanie jest niewykonalne.

`Aby stwierdzić czy liczba algebraiczna jest konstruowalna wystarczy znaleźć stopień jej wielomianu minimalnego. W rozstrzyganiu czy dany wielomian jest minimalny pomocne jest poniższe kryterium. Dowód prawdziwości tego kryterium pomijamy.

Kryterium Eisensteina

Wielomian postaci $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in Z[x]$ jest nierozkładalny jeśli istnieje liczba pierwsza *p*, taka, że *p* dzieli współczynniki $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ wielomianu i p^2 nie dzieli wyrazu wolnego a_0.

Zastosujmy kryterium Eisensteina do następującego przykładu.

Przykład 4.23

Liczba $a = \sqrt[5]{3+\sqrt{3}}$ jest pierwiastkiem wielomianu $W(x) = x^{10} - 6x^5 + 6$. Stosując kryterium Eisensteina dla wielomianu $W(x)$ i $p = 3$ stwierdzamy, że jest to wielomian nierozkładalny. Zatem stopień liczby *a* wynosi 10. Ponieważ 10 nie jest potęgą liczby 2, *a* jest niekonstruowalne.

Zauważmy, że to kryterium nie w każdym przypadku rozstrzyga czy wielomian jest rozkładalny czy nie. Dla wielomianu $V(x) = x^{10} - 6x^5 + 7$ kryterium nie daje nam odpowiedzi, więc nie wiemy jakiego stopnia jest liczba $b = \sqrt[5]{3+\sqrt{2}}$, będąca pierwiastkiem $V(x)$, a co za tym idzie nie wiemy czy jest konstruowalna.

O przydatności kryterium przekonamy się także w następnym rozdziale.

ZADANIA

Zad.4.1 Znajdź wielomiany o współczynnikach całkowitych, których pierwiastkmi są kolejno liczby: $\sqrt[4]{5}$, $\frac{1}{\sqrt{2}}$, $\sqrt{2}+\sqrt{3}$, $\sqrt{1+\sqrt{3}}$, $\frac{\sqrt{5}}{\sqrt[3]{4}}$, $\frac{1}{\sqrt{2}}+\sqrt{2}$.

Zad.4.2 Uzasadnij, że każda liczba algebraiczna stopnia 2 jest liczbą konstruowalną.

Zad.4.3 Wykonaj dzielenie (z resztą) wielomianu $x^3 - x^2 + 3x - 4$ przez wielomian $x^2 + 2x + 2$.

Zad.4.4 Sprawdź, że 1 jest pierwiastkiem wielomianu $x^3 - 2x^2 + 1$, a następnie przedstaw ten wielomian w postaci iloczynu $(x-1)\cdot Q(x)$.

Zad.4.5 Uzasadnij, że jeśli liczba *u* jest pierwiastkiem wielomianów $W_1(x)$ i $W_2(x)$. Zaś $P(x)$ i $Q(x)$ są dowolnymi wielomianami, to *u* jest też pierwiastkiem wielomianów $W_1(x)\cdot Q(x) - W_2(x)$, $[W_1(x) + W_2(x)]\cdot P(x) - Q(x)\cdot[W_2(x) - W_1(x)]$.

Zad.4.6 Przedstaw sumę, różnicę i iloczyn liczb $2 - \sqrt[3]{2} + 3\sqrt[3]{4}$ oraz $\sqrt[3]{4} - 7\sqrt[3]{2} + 5$ z ciała $Q(\sqrt[3]{2})$ w postaci $q_0 + q_1\sqrt[3]{2} + q_2(\sqrt[3]{2})^2$, gdzie q_0, q_1, q_2 są wymierne.

Zad.4.7 Niech u będzie pierwiastkiem wielomianu $x^3 - x^2 - 1$, oraz niech $a = 2 + u - 3u^2$, $b = 1 - u + u^2$. Przedstaw liczby $a\cdot b$ oraz $\frac{1}{a}$ w postaci $q_0 + q_1\sqrt[3]{2} + q_2(\sqrt[3]{2})^2$ gdzie q_0, q_1, q_2 są wymierne.

Zad.4.8 Znajdź stopień i bazę rozszerzenia $Q \subset Q(\sqrt[5]{2})$ jeśli wiadomo, że $\sqrt[5]{2}$ jest liczbą algebraiczną stopnia 5.

Zad.4.9 Niech $F_1 = Q(\sqrt{3})$ i $F_2 = F_1(\sqrt{5})$. Znajdź stopień i bazę rozszerzenia $Q \subset F_2$.

Zad.4.10 Znajdź wielomiany o współczynnikach całkowitych, których pierwiastkmi są kolejno liczby: $1 - \sqrt{2} + \sqrt{3}$, $1 + \sqrt[3]{2}$, $\sqrt[5]{3} - 1$, $\sqrt{2} + \sqrt[3]{2}$, $\frac{\sqrt{5}}{\sqrt[3]{2} - 1}$.

Zad.4.11 Uzasadnij, że liczby $\cos 10°$ oraz $\cos 18°$ są liczbami algebraicznymi. Wskazówka: zastosuj odpowiednią tożsamość trygonometryczną dla cosinusa odpowiedniej wielokrotności kąta.

Zad.4.12 Czy niewymierny pierwiastek czwartego stopnia z liczby wymiernej może być liczbą algebraiczną stopnia 2?

Zad.4.13 Zbadaj czy wielomian $2x^3 - 4x^2 + 3$ jest nierozkładalny nad *Q* (tzn. nie rozkłada się w iloczyn wielomianów o wymiernych współczynnikach).

Zad.4.14 Przedstaw liczby $\frac{1}{\sqrt[3]{2} - 1}$ oraz $\frac{1}{\sqrt[3]{2} - \sqrt[3]{4} + 1}$ w postaci $q_0 + q_1\sqrt[3]{2} + q_2\sqrt[3]{4}$, gdzie $q_0, q_1, q_2 \in Q$.

Zad.4.15 Znajdź wielomian stopnia 3 o całkowitych współczynnikach, którego pierwiastkiem jest liczba $a = \sqrt[3]{2} - \sqrt[3]{4}$. Sprawdź, że jest to wielomian minimalny tej liczby. Wskazówka: przedstaw liczby a^2 i a^3 w wiadomej postaci właściwej rozszerzenia $Q(\sqrt[3]{2})$, a następnie

znajdź kombinację liniową liczb 1, a, a^2 równą liczbie a^3; dla dowodu minimalności sprawdź, że otrzymany wielomian jest nierozkładalny.

Zad.4.16 Znajdź wielomian stopnia 2 o całkowitych współczynnikach, którego pierwiastkiem jest liczba $3-2\sqrt{2}$, a następnie uzasadnij, że jest to wielomian minimalny tej liczby. Wskazówka: zastosuj np. metodę z poprzedniego zadania.

Zad.4.17 Korzystając z tego, że $\sqrt[3]{2}$ jest niekonstruowalny, oraz stosując rozumowanie nie wprost uzasadnij, że liczba $2\sqrt[3]{4}+\sqrt[3]{2}-1$ jest niekonstruowalna. Wywnioskuj stąd (bez znajdowania wielomianu minimalnego), że stopień tej liczby wynosi 3.

Zad.4.18 Niech $F_1 = Q\left(\sqrt{2}\right)$, $F_2 = F_1\left(\sqrt{3}\right)$ i $F_3 = F_2\left(\sqrt{\sqrt{2}+\sqrt{3}}\right)$. Znajdź stopień i bazę rozszerzenia $Q \subset F_3$.

Zad.4.19 Sprawdź, że rozszerzenie $Q\left(1+\sqrt{5}\right)$ ciała Q o liczbę algebraiczną $1+\sqrt{5}$ jest dokładnie tym samym ciałem co rozszerzenie kwadratowe $Q\left(\sqrt{5}\right)$.

Zad.4.20 Uzasadnij, że każde rozszerzenie stopnia 2 jest rozszerzeniem kwadratowym.

Zad.4.21 Uzasadnij, że jeśli $W(x)$ jest wielomianem minimalnym niewymiernej liczby algebraicznej u, to W nie posiada żadnego pierwiastka wymiernego.

Zad.4.22 Uzasadnij, że jeśli u jest liczbą algebraiczną stopnia k, zaś x jest różnym od u pierwiastkiem wielomianu minimalnego liczby u, to x jest też liczbą algebraiczną stopnia k.

Zad.4.23 Podaj pełną charakteryzację liczb algebraicznych stopnia 2.

Zad.4.24 Czy za pomocą cyrkla i linijki jest wykonalna konstrukcja koła o polu równym

(a) polu danego kwadratu (jest to problem odwrotny do problemu kwadratury koła);
(b) połowie pola danego koła;
(c) sumie pól dwóch danych kół?

Zad.4.25 Czy za pomocą cyrkla i linijki jest wykonalna konstrukcja

(a) koła o obwodzie równym danemu odcinkowi;
(b) koła o obwodzie równym sumie obwodów trzech danych kół;
(c) półkola o obwodzie równym danemu odcinkowi;
(d) półkola o obwodzie równym obwodowi danego koła?

Zad.4.26 O których z poniższych wielomianów potrafisz rozstrzygnąć, że są nierozkładalne bezpośrednio stosując kryterium Eisenteina:

$x^4+6x^2-18x+12$, $x^4+21x^3-3x^2+49$, x^5-10x^3+50 ?

Zad.4.27 Znajdź wielomian minimalny liczby $\sqrt[3]{2+\sqrt{6}}$.

Zad.4.28 Znajdź stopień liczby algebraicznej $\sqrt{3-\sqrt[4]{3}}$.

Zad.4.29 Dla jakich liczb naturalnych *k* można uzasadnić stosując bezpośrednio kryterium Eisensteina, że $\sqrt[n]{k}$ jest liczba algebraiczną stopnia *n* ?

Zad.4.30 Uzasadnij, że jeśli wielomian $W(x) \in Q[x]$ jest nierozkładalny nad *Q*, zaś *q* jest liczbą wymierną różną od zera, to wielomian $W(x+q)$ jest też nierozkładalny nad *Q*.

Zad.4.31 Uzasadnij, że liczba $\sqrt[5]{36}$ jest liczbą algebraiczną stopnia 5. Wskazówka: rozważ wielomian $W'(x) := W(x+1)$ dla wielomianu $W(x) = x^5 - 36$.

Podobnym sposobem uzasadnij, że stopień liczby $\sqrt[5]{4}$ wynosi 5.

Zad.4.32 Uzasadnij, że jeśli *u* jest liczbą algebraiczną, zaś $q \in Q$, to $st(u+q) = st(u)$. Wskazówka: rozważ wielomian minimalny $W(x)$ liczby *u* oraz wielomian $W(x-q)$.

Zad.4.33 Uzasadnij, że jeśli wielomian $W(x) \in Q[x]$ jest nierozkładalny nad *Q*, zaś *q* jest liczbą wymierną różną od zera, to wielomian $W(q \cdot x)$ jest też nierozkładalny nad *Q*.

Wywnioskuj stąd, że dla dowolnej liczby algebraicznej *u* oraz wymiernej *q* stopnie liczb $u \cdot q$ oraz *u* są równe.

Zad.4.34 Uzasadnij, że wielomian $W(x) = 2x^4 - 7$ jest nierozkładalny, rozważając wielomian $W\left(\frac{x}{2}\right)$ pomnożony przez taką liczbę, by współczynniki stały się całkowite.

Podobnie uzasadnij, że nierozkładalny jest wielomian $9x^5 + 5$.

Zad.4.35 Znajdź stopień liczby $\sqrt[5]{3/2}$ dwoma sposobami:

(a) Korzystając z tego, że $\sqrt[5]{3/2} = \frac{1}{2}\sqrt[5]{48}$ oraz z zadania 4.33;

(b) Posługując się metodą z zadania 4.34.

Podobnie znajdź stopień liczby $\sqrt[4]{2/3}$.

Zad.4.36 Dla danego wielomianu $W(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ rozważmy wielomian $\overset{\circ}{W}(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$

(a) Uzasadnij, że $\overset{\sigma}{W}(x) = x^{st(W)} \cdot W\left(\frac{1}{x}\right)$.

(b) Uzasadnij, że jeśli liczba $u \neq 0$ jest pierwiastkiem W, to liczba $\frac{1}{u}$ jest pierwiastkiem $\overset{\circ}{W}$.

(c) Uzasadnij, że jeśli $W(x) = W_1(x) \cdot W_2(x)$, to $\overset{\circ}{W}(x) = \overset{\circ}{W}_1(x) \cdot \overset{\circ}{W}_2(x)$.

(d) Uzasadnij, że jeśli W jest nierozkładalny, to $\overset{\circ}{W}$ też.

(e) Wywnioskuj, że dla dowolnej liczby algebraicznej $u \neq 0$ $st\left(\frac{1}{u}\right) = st(u)$.

(f) Znajdź stopień liczby $\sqrt[5]{9/5}$.

Zad.4.37 $W(x) = x^3 - 15x^2 + 12$ jest wielomianem minimalnym liczby algebraicznej u. Znajdź wielomiany minimalne liczb $u-2$, $3u$, $\frac{2}{5}u$, $2u+3$, $\frac{1}{u}$, $\frac{1}{u+|1}$, $\frac{2}{2u-1}$, $\frac{u-1}{u+1}$.

ROZDZIAŁ V

Liczby zespolone konstruowalne.

Do tej pory zajmowaliśmy się liczbami konstruowalnymi rzeczywistymi. Przenieśmy teraz nasze rozważania na płaszczyznę zespoloną.

Zdefiniujmy najpierw ciało liczbowe zespolone.

Definicja 5.1

Ciałem liczbowym zespolonym nazywamy dowolne podciało ciała wszystkich liczb zespolonych.

Równoważnie możemy opisać ciało liczbowe zespolone jako dowolny zbiór L liczb zespolonych taki, że jeśli x i y są elementami L to liczby $x+y, x-y, xy$ oraz $\frac{x}{y}$ (dla y różnych od zera) też należą do L.

Przyjrzyjmy się przykładowi ciała liczbowego zespolonego.

Przykład 5.2

Przykładem ciała liczbowego zespolonego jest zbiór $L=\{a+bi : a,b \in Q\}$. Sprawdźmy, że tak zdefiniowany zbiór L rzeczywiście jest ciałem. Weźmy dwa elementy należące do L : $x=a+bi$ oraz $y=c+di$ (a, b, c, d są wymierne). Suma $x+y$ jest postaci $(a+c)+(b+d)i$, gdzie $a+c, b+d$ są wymierne więc należy do L. Podobnie różnica $x-y$ ma postać $(a-c)+(b-d)i$ gdzie $a-c, b-d$ są wymierne, więc także należy do L. Dla iloczynu $xy=(a+bi)(c+di)$, po wymnożeniu nawiasów i wykorzystaniu faktu, że i^2 wynosi –1, ostatecznie otrzymujemy postać $(ac-bd)+(ad+bc)i$, gdzie $ac-bd$ oraz $ad+bc$ są wymierne, więc iloczyn xy należy do L. Zamiast ilorazu wystarczy pokazać, że element odwrotny x, postaci $\frac{1}{a+bi}$, należy do L. Mnożąc element odwrotny przez wyrażenie $\frac{a-bi}{a-bi}$ otrzymujemy $\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i$. Współczynniki $\frac{a}{a^2+b^2}$ i $\frac{b}{a^2+b^2}$ są wymierne, zatem element odwrotny należy do L. Tym sposobem pokazaliśmy, że zbiór $L=\{a+bi : a,b \in Q\}$ jest ciałem.

Dla ciała liczbowego zespolonego możemy także wprowadzić definicją rozszerzenia kwadratowego zespolonego.

Definicja 5.3

Niech F będzie ciałem liczbowym zespolonym i niech a będzie elementem ciała F takim, że $\sqrt{a}$ nie należy do F. Wtedy zbiór $F_1 = \{x + y\sqrt{a} : x, y \in F\}$ nazywamy rozszerzeniem kwadratowym zespolonym.

Zdefiniowany powyżej zbiór F_1 nie zależy od wyboru pierwiastka spośród dwóch pierwiastków liczby a, czyli zachodzi równość $F_1(\sqrt{a}) = F_1(-\sqrt{a})$.

Zauważmy, że zespolone rozszerzenie kwadratowe również jest ciałem. Fakt ten uzasadnia się tak samo jak w przypadku rozszerzenia kwadratowego rzeczywistego z rozdziału II (dowód lematu 2.4).

Przykładem rozszerzenia kwadratowego zespolonego na mocy definicji 5.3 może być zbiór $L = \{a + bi : a, b \in Q\}$ z przykładu 5.2, ponieważ $L = Q(\sqrt{-1})$.

Zdefiniujmy teraz liczby zespolone konstruowalne. Możemy wprowadzić trzy równoważne definicje.

Definicja 5.4.1

Liczba zespolona z jest konstruowalna jeśli z jest punktem płaszczyzny dającym się skonstruować za pomocą cyrkla i linijki wychodząc od punktów (0,0) i (1,0).

Definicja 5.4.2

Liczba zespolona z jest konstruowalna jeśli z jest postaci $a + bi$, gdzie a i b są konstruowalne.

Definicja 5.4.3

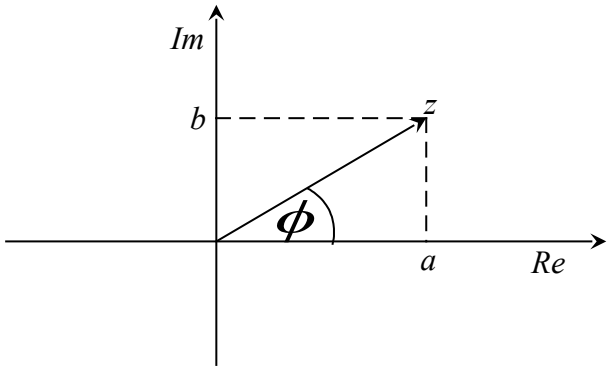
Liczba zespolona z jest konstruowalna jeśli istnieje ciąg rozszerzeń kwadratowych zespolonych $Q = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n$ taki, że $z \in F_n$.

Równoważność definicji 5.4.1 i definicji 5.4.2 wynika z naszych rozważań z rozdziału pierwszego, gdzie punkty dające się skonstruować na płaszczyźnie były punktami o obu współrzędnych konstruowalnych.

Uzasadnijmy więc równoważność definicji 5.4.2 i definicji 5.4.3. W tym celu posłużymy się lematem.

Lemat 5.5

Niech liczba $z = a + bi$ przedstawia się równoważnie w postaci $r(\cos\phi + i\sin\phi)$. Wtedy konstruowalność liczb *a* i *b* jest równoważna konstruowalności liczby *r* oraz kąta ϕ.



Rysunek 4

Dowód

$(\Rightarrow)$ Załóżmy, że liczby *a* i *b* są konstruowalne. Wiemy, że liczba *r* jest równa $|z|$ (rys.1), czyli liczbie $\sqrt{a^2 + b^2}$, zatem jest konstruowalna. Konstruowalnośc kąta ϕ jest równoważna konstruowalności liczby $\cos\phi$. Ponieważ $\cos\phi$, jak widać na rysunku 1, wynosi $\frac{a}{r}$ więc jest konstruowalny.

$(\Leftarrow)$ Załóżmy, że liczby *r* i $\cos\phi$ są konstruowalne. Wtedy liczba *a* równa liczbie $r\cos\phi$ jest konstruowalna oraz liczba *b* równa liczbie $r\sin\phi$ (rys.1), czyli liczbie $\pm r\sqrt{1-\cos^2\phi}$ jest konstruowalna.

Teraz możemy przystąpić do dowodu, że definicje 5.4.2 i 5.4.3 są równoważne.

Dowód

Pokażemy, że z definicji 5.4.2 wynika definicja 5.4.3. Weźmy więc liczbę *z* postaci $a + bi$, gdzie *a* i *b* są konstruowalne. Istnieją zatem ciągi rozszerzeń kwadratowych (rzeczywistych) dla *a* kolejno o pierwiastki $\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}$ i dla *b* o pierwiastki $\sqrt{\beta_1}, \sqrt{\beta_2}, \ldots, \sqrt{\beta_m}$. Utwórzmy ciąg rozszerzeń zespolonych dla liczby $z = a + bi$. Mamy więc następujący ciąg

$$Q = F_0 \subset F_1 = F_0\left(\sqrt{\alpha_1}\right) \subset F_2 = F_1\left(\sqrt{\alpha_2}\right) \subset \ldots \subset F_n = F_{n-1}\left(\sqrt{\alpha_n}\right) \subset F_{n+1} = F_n\left(\sqrt{\beta_1}\right) \subset$$

$$\subset F_{n+2} = F_{n+1}\left(\sqrt{\beta_2}\right) \subset \ldots \subset F_{n+m} = F_{n+m-1}\left(\sqrt{\beta_m}\right) \subset F_{n+m+1} = F_{n+m}(i).$$

Każde z tych rozszerzeń jest rozszerzeniem kwadratowym. Niektóre rozszerzenia mogą być trywialne, wtedy powyższy ciąg w rzeczywistości będzie krótszy, nie ma to jednak wpływu na nasze rozważania. Ponieważ liczby *a, b, i* należą do F_{n+m+1}, więc liczba $z = a + bi$ też należy do tego rozszerzenia, czyli jest konstruowalna.

Musimy jeszcze pokazać implikację odwrotną czyli, że z definicji 5.4.3 wynika definicja 5.4.2. Mamy daną konstruowalną liczbę $z = a + bi$ i jej ciąg rozszerzeń $Q = F_0 \subset F_1 \subset \ldots \subset F_{n-1} \subset F_n$, mamy pokazać, że liczby *a* i *b* są konstruowalne. Wystarczy uzasadnić, że jeśli każdy $x \in F_k$ ma część rzeczywistą i urojoną konstruowalną, to każdy $y \in F_{k+1}$ też. Zauważmy, że rozszerzenie F_{k+1} jest zbiorem postaci $F_{k+1} = \left\{a + b\sqrt{c} : a,b,c \in F_k\right\}$. Pozostaje nam więc pokazać, że część rzeczywista i urojona liczby $\sqrt{c}$ jest konstruowalna. Liczbę *c* możemy zapisać w postaci trygonometrycznej $r(\cos\phi + i\sin\phi)$ (r, ϕ konstruowalne ponieważ *c* jest konstruowalna), wtedy $\sqrt{c}$ możemy przedstawić ze wzoru de Moivre'a jako $\sqrt{r}\left(\cos\frac{\phi}{2} + i\sin\frac{\phi}{2}\right)$. Ponieważ *r* i ϕ są konstruowalne, to $\sqrt{r}$ i $\frac{\phi}{2}$ też. Zatem na mocy lematu 5.5 część rzeczywista i część urojona liczby $\sqrt{c}$ są konstruowalne, więc tak samo część rzeczywista i urojona każdego *y* z F_{k+1} są konstruowalne. Zaczynając od ciała F_0 i przeprowadzając indukcyjnie powyższe rozumowanie ostatecznie otrzymujemy, że część rzeczywista i urojona liczby *z* (czyli *a* i *b*) są konstruowalne.

Z przechodniości relacji równoważności wynika, że definicja 5.4.1 jest równoważna definicji 5.4.3, zatem wszystkie trzy definicje liczb zespolonych konstruowalnych są równoważne.

Dla liczb zespolonych, podobnie jak dla liczb rzeczywistych, wprowadźmy definicję algebraiczności.

Definicja 5.6

Liczba zespolona *z* jest algebraiczna jeśli jest pierwiastkiem pewnego wielomianu $W(x) \in Q[x]$.

Dla liczb algebraicznych zespolonych zachodzą te same fakty co dla liczb algebraicznych rzeczywistych, mianowicie:

- wielomian minimalny liczby algebraicznej jest jednoznacznie wyznaczony (z dokładnością do wymiernego czynnika);
- wielomian minimalny jest nierozkładalny nad ciałem *Q*;
- taki sam opis rozszerzenia ciała *Q* o zespoloną liczbę algebraiczną jak w przypadku rzeczywistym.

Stopień liczby algebraicznej zespolonej, tak jak rzeczywistej, jest równy stopniowi jej wielomianu minimalnego. Tak samo jak dla ciał rzeczywistych definiuje się również bazę i stopień rozszerzenia dla zespolonych ciał liczbowych.

W związku z tym możemy również wyciągnąć wniosek (analogiczny do wniosku 4.19).

Wniosek 5.7

Każda zespolona liczba konstruowalna jest liczbą algebraiczną, a jej stopień jest potęgą liczby 2. Zespolona liczba algebraiczna stopnia różnego niż 2^k nie jest konstruowalna.

Zebraną wiedzę o liczbach zespolonych konstruowalnych wykorzystamy w następnym rozdziale do rozwiązania problemu konstruowalności *n*-kątów foremnych.

ZADANIA

Zad.5.1 Niech $ax^2+bx+c \in Q[x]$ ma wyróżnik Δ ujemny i niech ξ będzie jego pierwiastkiem. Uzasadnij, że $Q(\xi)=\left\{a+b\sqrt{-\Delta}\,i : a,b \in Q\right\}$.

Zad.5.2 Znajdź wielomiany minimalne liczb algebraicznych:

$$z=i+\sqrt{2}\,, \quad u=1-\sqrt[3]{3}+\sqrt[3]{9}, \quad w=\sqrt{6}-i\sqrt{3}\,.$$

Zad.5.3 Czy pierwiastki zespolone wielomianu x^4+2x^2+4 są konstruowalne? A jak będzie dla dowolnego innego wielomianu postaci $x^4+ax^2+b \in Q[x]$?

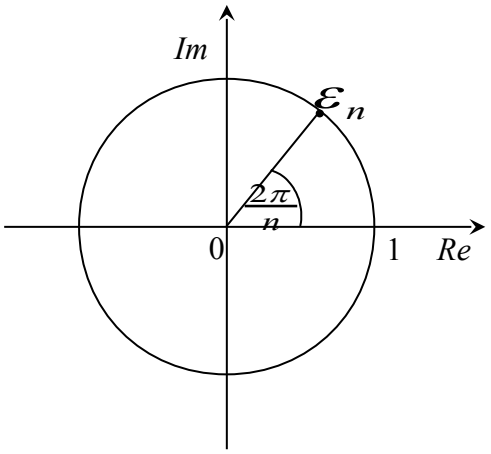
Zad.5.4 Znajdź wszystkie zespolone liczby algebraiczne stopnia 2 (podaj ich ogólną postać).

ROZDZIAŁ VI

Konstruowalność *n*-kątów foremnych.

W ostatnim rozdziale zajmiemy się konstruowalnością *n*-kątów foremnych. Znajdziemy liczby *n*, dla których *n*-kąt jest konstruowalny i takie dla których jest niekonstruowalny. W tym celu posłużymy się liczbami konstruowalnymi zespolonymi.

Zauważmy, ze konstruowalność *n*-kąta foremnego jest równoważna konstruowalności *n*-tego pierwotnego pierwiastka z jedności, czyli liczby $\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ (rys. 2).



Rysunek 5

Mając dany *n*-kąt foremny oraz punkty $(0,0)$ i $(1,0)$ skonstruujemy pierwiastek ε_n, wyznaczając kąt $\frac{2\pi}{n}$ z *n*-kąta i przenosząc go na płaszczyznę zespoloną tak, by jego wierzchołek znajdował się w punkcie $(0,0)$, a jedno ramię pokrywało się z osią rzeczywistą. Rysując okrąg jednostkowy o środku w $(0,0)$ otrzymamy ε_n, który jest punktem przecięcia okręgu i ramienia kąta nie pokrywającego się z osią rzeczywistą. Natomiast mając daną liczbę ε_n oraz punkty $(0,0)$ i $(1,0)$ skonstruujemy *n*-kąt foremny odkładając odcinek $\overline{1\varepsilon_n}$ na okręgu jednostkowym.

Liczba ε_n jest liczbą algebraiczną, ponieważ jest pierwiastkiem wielomianu $W(x) = x^n - 1$. Zatem żeby stwierdzić czy ε_n jest konstruowalna (czyli czy *n*-kąt jest konstruowalny) musimy zbadać jej stopień. Ponieważ liczba 1 jest pierwiastkiem $W(x)$, to dzieląc wielomian $W(x)$ przez $x-1$ otrzymujemy $x^{n-1} + x^{n-2} + \ldots + x + 1 = W_n(x)$. Zatem liczba ε_n musi być

pierwiastkiem wielomianu $W_n(x)$. Sprawdźmy dla jakich n wielomian $W_n(x)$ jest nierozkładalny nad Q.

Stwierdzenie 6.1

Jeśli n jest liczbą złożoną, to wielomian $W_n(x)$ jest rozkładalny nad Q.

Dowód

Niech n przedstawia się w postaci iloczynu kl. Wtedy wielomian $W_n(x)=x^{n-1}+x^{n-2}+\ldots+x+1$ jest rozkładalny i ma rozkład postaci $W_n(x)=\left(x^{l-1}+x^{l-2}+\ldots+x+1\right)\left(x^{(k-1)l}+x^{(k-2)l}+\ldots+x^{l}+1\right)$.

Stwierdzenie 6.2

Jeśli p jest liczbą pierwszą to wielomian $W_p(x)$ jest nierozkładalny nad Q.

Dowód

Nierozkładalność wielomianu $W_p(x)=x^{p-1}+x^{p-2}+\ldots+x+1$ jest równoważna nierozkładalności wielomianu $W'(x)=W_p(x+1)$ (porównaj zadanie 4.30). Wystarczy więc uzasadnić nierozkładalność wielomianu $W'(x)$. Wielomian $W'(x)$ otrzymamy z ilorazu $\frac{(x+1)^p-1}{(x+1)-1}=\frac{(x+1)^p-1}{x}$. Stosując dwumian Newtona do $(x+1)^p$ dostajemy wyrażenie postaci $\left(x^p+\binom{p}{1}x^{p-1}+\binom{p}{2}x^{p-2}+\ldots+\binom{p}{p-1}x+1-1\right)\cdot\frac{1}{x}$. Ostatecznie otrzymujemy wielomian $W'(x)=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\ldots+\binom{p}{p-1}$. Zastosujmy kryterium Eisensteina z użyciem liczby pierwszej p. Musimy uzasadnić, że dla $k=1,2,\ldots,p-1$ wyrażenie jest podzielne przez p. Zauważmy, że w rozkładzie licznika na czynniki pierwsze występuje liczba pierwsza p, natomiast w rozkładzie mianownika p nie występuje. Zatem po redukcji licznika i mianownika czynnik p zostanie, więc dla danych k z pewnością dzieli się przez p.

Liczba $\binom{p}{p-1} = p$ nie dzieli się przez p^2. Na mocy kryterium Eisensteina wielomian $W'(x)$ jest nierozkładalny, czyli wielomian $W_p(x)$ też.

Z powyższego stwierdzenia i do tej pory zdobytych wiadomości możemy wyciągnąć wnioski.

Wniosek 6.3

Wielomian $W_p(x)$ jest wielomianem minimalnym dla liczby $\varepsilon_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Zatem stopień liczby ε_p wynosi $p-1$.

Wniosek 6.4

Jeśli p jest liczbą pierwszą taką, że $p-1 \neq 2^k$ to liczba ε_p jest niekonstruowalna (wówczas nie istnieje również konstrukcja p-kąta foremnego). Jeśli zaś stopień ε_p jest potęgą liczby 2 to liczba ε_p jest konstruowalna (więc konstruowalny jest także p-kąt foremny).

Rozstrzygnijmy konstruowalność p-kątów foremnych dla niektórych liczb pierwszych p.

Przykład 6.5

- Dla p=7 mamy $p-1=6$, ponieważ $6 \neq 2^k$, więc 7-kąt jest niekonstruowalny (niekonstruowalność 7-kąta uzasadniliśmy już w przykładzie 3.7 stosując inne metody).
- Dla p=11 mamy $p-1=10$, ponieważ $10 \neq 2^k$, więc 11-kąt jest niekonstruowalny.
- Dla p=13 mamy $p-1=12$, ponieważ $12 \neq 2^k$, więc 13-kąt jest niekonstruowalny.
- Dla p=3 mamy $p-1=2=2^1$, zatem trójkąt jest konstruowalny (konstruowalność trójkąta jest skądinąd oczywista).
- Dla p=5 mamy $p-1=4=2^2$, zatem pięciokąt jest konstruowalny (konstrukcja pięciokąta patrz zad.1.11(c)).
- Dla p=17 mamy $p-1=16=2^4$, zatem 17-kąt jest konstruowalny.
- Dla p=257 mamy $p-1=256=2^8$, zatem 257-kąt jest konstruowalny.

- Dla p=65537 mamy $p-1=65536=2^{16}$, zatem 65537-kąt jest konstruowalny.

Liczby pierwsze p takie, że $p-1$ jest postaci 2^k nazywane są liczbami pierwszymi Fermata. Dotychczas nie udowodniono czy istnieją liczby pierwsze Fermata różne od wymienionych w powyższym przykładzie.

Dodatkowym wyznacznikiem konstruowalności wielokątów foremnych jest poniższe twierdzenie.

Twierdzenie 6.6

Jeśli p jest liczbą pierwszą różną od 2, to p^2-kąt foremny jest niekonstruowalny.

Dowód

Wystarczy uzasadnić, że pierwiastek $\varepsilon_{p^2}=\cos\frac{2\pi}{p^2}+i\sin\frac{2\pi}{p^2}$ jest liczbą zespoloną niekonstruowalną, a zatem wystarczy uzasadnić, że stopień liczby ε_{p^2} nie jest potęgą liczby 2. Liczba ε_{p^2} jest pierwiastkiem wielomianu $\frac{x^{p^2}-1}{x-1}=x^{p^2-1}+x^{p^2-2}+\ldots+x+1$. Wielomian ten jest rozkładalny i jego rozkład jest postaci

$$\left(x^{p-1}+x^{p-2}+\ldots+x+1\right)\left(x^{(p-1)p}+x^{(p-2)p}+\ldots+x^p+1\right).$$

Liczba ε_{p^2} nie jest pierwiastkiem czynnika $x^{p-1}+\ldots+x+1=\frac{x^p-1}{x-1}$, ponieważ pierwiastkami tego wielomianu są liczby postaci $\cos\left(\frac{2\pi}{p}k\right)+i\sin\left(\frac{2\pi}{p}k\right)$ dla $k=1,\ldots,p-1$. Zatem ε_{p^2} musi być pierwiastkiem wielomianu $x^{(p-1)p}+\ldots+x^p+1$. Uzasadnijmy, że wielomian ten jest nierozkładalny.

Nierozkładalność wielomianu $V(x)$ jest równoważna nierozkładalności wielomianu $V'(x)=V(x+1)$ (porównaj zadanie 4.30). zauważmy również, że dla wielomianu $V(x)$ zachodzi równość $V(x)=W_p(x^p)$, gdzie $W_p(x)$ jest wielomianem postaci

$$x^{p-1}+x^{p-2}+\ldots+x+1.$$

Mamy zatem następujący ciąg równości $V'(x)=V(x+1)=W_p\left((x+1)^p\right)=W_p\left(\sum_{i=1}^{p}\binom{p}{i}x^i+1\right)$.

Przyjmijmy, że $\sum_{i=1}^{p}\binom{p}{i}x^i = y$. Na podstawie wcześniejszych obliczeń przeprowadzonych w dowodzie stwierdzenia 6.2 otrzymujemy

$$V(x+1) = W_p(y+1) = y^{p-1} + \sum_{j=2}^{p-1}\binom{p}{j}y^{j-1} + p = \left(x^p + \sum_{i=1}^{p-1}\binom{p}{i}x^i\right)^{p-1} + \sum_{j=2}^{p-1}\binom{p}{j}\left(\sum_{i=1}^{p}\binom{p}{i}x^i\right)^{j-1} + p\,.$$

W otrzymanym wielomianie najwyższy współczynnik wynosi 1, pozostałe dzielą się przez *p*, a wyraz wolny jest równy *p*. Stosując kryterium Eisensteina z użyciem liczby pierwszej *p* stwierdzamy, że wielomian $V(x+1)$ jest nierozkładalny, czyli wielomian $V(x)$ też.

Stopień liczby ε_{p^2} jest więc równy $(p-1)p$. Jeżeli *p* jest liczbą pierwszą różną od 2 to liczba $(p-1)p$ nie może być potęgą liczby 2. Stąd stopień ε_{p^2} nie jest postaci 2^k, więc p^2-kąt nie jest konstruowalny.

Zauważmy, że z dowolnego konstruowalnego *n*-kąta foremnego możemy otrzymać konstrukcję 2*n*-kąta foremnego połowiąc łuki koła opisanego odpowiadające każdemu bokowi *n*-kąta i wykorzystując znalezione w ten sposób punkty jako dodatkowe wierzchołki dla szukanego 2*n*-kąta. Zaczynając wiec od średnicy koła możemy skonstruować 4-kąt, 8-kąt, 16-kąt, ..., 2*n*-kąt. Podobnie możemy otrzymać 6-kąt, 12-kąt, 24-kąt, 48-kąt, itd. z trójkąta oraz 20-kąt, 40-kąt, itd. z 10-kąta (konstruowalność 10-kąta uzasadniliśmy w przykładzie 1.9). Podobnie mając dany 2*n*-kąt foremny możemy skonstruować *n*-kąt foremny biorąc co drugi wierzchołek 2*n*-kąta i wykorzystując otrzymane punkty jako wierzchołki *n*-kąta (np. 5-kąt z 10-kąta).

Jeśli *n*-kąt foremny jest niekonstruowalny, to dla każdej liczby naturalnej *m*, *mn*-kąt foremny też jest niekonstruowalny (gdyby *mn*-kąt był konstruowalny to biorąc co *m*-ty wierzchołek mielibyśmy konstrukcję *n*-kąta). Czyli z niekonstruowalności 7-kąta foremnego (uzasadniliśmy ją w przykładzie 3.7) wynika niekonstruowalność 14-kąta, 21-kąta, 28-kąta itd.

Dodatkowo dla wielokątów foremnych zachodzi poniższe stwierdzenie.

Stwierdzenie 6.7

Jeśli *m, n* są względnie pierwsze oraz *m*-kąt i *n*-kąt są konstruowalne, to *mn*-kąt też jest konstruowalny.

Dowód

Z założenia wiemy, że *n*-kąt i *m*-kąt są konstruowalne, czyli konstruowalne są kąty $\frac{2\pi}{n}$ i $\frac{2\pi}{m}$. Wystarczy więc pokazać, że przy pomocy kątów $\frac{2\pi}{n}$ i $\frac{2\pi}{m}$ można skonstruować kąt $\frac{2\pi}{mn}$. Musimy znaleźć takie liczby całkowite *a* i *b* dla których zachodzi równość $\frac{2\pi}{mn} = a \cdot \frac{2\pi}{m} + b \cdot \frac{2\pi}{n}$. Warunek ten jest równoważny warunkowi $an + bm = 1$. Z twierdzeń arytmetyki wynika, że jeśli *m* i *n* są względnie pierwsze to istnieją liczby *a* i *b* dla których $an + bm = 1$. Zatem istnieje konstrukcja kąta $\frac{2\pi}{mn}$, co jest równoważne konstruowalności *mn*-kąta foremnego.

Przekonajmy się jak działa powyższe stwierdzenie na przykładzie.

Przykład 6.8

Uzasadnijmy, że istnieje konstrukcja 15-kąta. Zauważmy, że liczba 15 jest iloczynem liczb 3 i 5, gdzie 3 i 5 są względnie pierwsze. Trójkąt i pięciokąt są konstruowalne, więc kąty $\frac{2\pi}{3}$ i $\frac{2\pi}{5}$, będące odpowiednio kątami trójkąta i pięciokąta, też. Pokażemy, że mając dane kąty $\frac{2\pi}{3}$ i $\frac{2\pi}{5}$ możemy skonstruować kąt $\frac{2\pi}{15}$. Zapiszmy ułamki $\frac{2\pi}{3}$ i $\frac{2\pi}{5}$ w postaci ułamków o mianowniku 15, czyli $\frac{2\pi}{3} = \frac{10\pi}{15}$ oraz $\frac{2\pi}{5} = \frac{6\pi}{15}$. Ponieważ prawdziwa jest następująca równość $\frac{2\pi}{15} = 2 \cdot \frac{6\pi}{15} - \frac{10\pi}{15}$, więc potrafimy skonstruować kąt $\frac{2\pi}{15}$ przy pomocy danych kątów, co jest równoważne konstruowalności 15-kąta.

Konstruowalność dowolnych *n*-kątów foremnych – ostateczne wnioski.

Niech liczba *n* ma rozkład na czynniki pierwsze postaci $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$, wtedy zachodzą poniższe fakty.

Fakt 6.8

Dla $p_i \neq 2$, jeśli którykolwiek wykładnik n_i jest większy od 1 to *n*-kąt jest konstruowalny;

Dowód

Załóżmy, że wykładnik n_1 jest większy od 1. Wtedy mamy $n = p_1^2\left(p_1^{n_1-2} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}\right)$. Iloczyn $p_1^{n_1-2} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ jest pewną liczbą naturalną *m*. Na mocy twierdzenia 6.6 p_1^2-kąt foremny jest niekonstruowalny. Wiemy również, że jeśli p_1^2-kąt jest niekonstruowalny to dla każdej liczby naturalnej *m*, mp_1^2-kąt foremny też jest niekonstruowalny. Zatem nie istnieje konstrukcja *n*-kąta foremnego, gdzie $n = mp_1^2$.

Fakt 6.9

Jeśli występuje czynnik pierwszy p_i nie będący liczbą Fermata to *n*-kąt jest niekonstruowalny.

Dowód

Załóżmy, że czynnik p_1 nie jest liczbą Fermata, czyli $p - 1 \neq 2^k$.
Na mocy wniosku 6.4 stwierdzamy, że p_1-kąt jest niekonstruowalny więc mp_1-kąt foremny, gdzie $m = p_1^{n_1-1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ jest liczbą naturalną, także nie daje się skonstruować. Nie istnieje zatem konstrukcja *n*-kąta foremnego, gdzie $n = mp_1$.

Fakt 6.10

Jeśli rozkład liczby *n* jest postaci $n = 2^k \cdot p_1 \cdot \ldots \cdot p_n$, gdzie p_i są parami różnymi liczbami pierwszymi Fermata to *n*-kąt jest konstruowalny.

Dowód

Z wniosku 6.4 wiemy, że p_1-kąt foremny, ..., p_n-kąt foremny są konstruowalne. Zauważmy, że liczby $p_1, \ldots, p_n$ są parami względnie pierwsze. Stosując stwierdzenie 6.7 dla liczb $p_1, \ldots, p_n$ otrzymujemy, że $p_1 \cdot \ldots \cdot p_n$-kąt jest konstruowalny. Z wcześniejszych rozważań wiemy, że z dowolnego konstruowalnego *m*-kąta możemy otrzymać konstrukcję 2*m*-kąta foremnego, więc także $2^k m$-kąta foremnego. Pokazaliśmy zatem, że istnieje konstrukcja *n*-kąta foremnego, gdzie $n = 2^k \cdot p_1 \cdot \ldots \cdot p_n$.

Ponieważ powyższe trzy przypadki wyczerpują wszystkie możliwe rozkłady liczby *n* na czynniki,prawdziwe jest następujące stwierdzenie.

Stwierdzenie 6.11

Jedynymi *n*-kątami foremnymi konstruowalnymi za pomocą cyrkla i linijki są *n*-kąty dla których rozkład *n* jest postaci $n = 2^k \cdot p_1 \cdot \ldots \cdot p_n$, gdzie $k \geq 0$, a p_i są parami różnymi liczbami pierwszymi Fermata.

ZADANIA

Zad.6.1 Uzasadnij, że jeśli *p* jest nieparzystą liczbą pierwszą, zaś $E_{2p} = \cos\frac{2\pi}{2p} + i \cdot \sin\frac{2\pi}{2p}$ jest pierwotnym *2p* – tym pierwiastkiem z 1, to $st(E_{2p}) = p - 1$, w następujących krokach:

(a) E_{2p} jest pierwiastkiem wielomianu $x^p + 1$;

(b) E_{2p} jest pierwiastkiem wielomianu $Z(x) = \frac{x^p + 1}{x + 1}$;

(c) wielomian $Z(x)$ jest nierozkładalny, bo wielomian

$Z'(x) = Z(x-1) = \frac{(x-1)^p + 1}{(x-1)+1} = \frac{(x-1)^p + 1}{x}$ jest nierozkładalny;

(d) ostateczne konkluzje.

Zad.6.2 Przyjmując, że wiemy jak skonstruować 17–kąt foremny, podaj konstrukcję 34–kąta, 51–kąta i 85-kąta foremnego.

Zad.6.3 Spośród liczb naturalnych od 3 do 100 wykreśl (lub wypisz) te liczby *n*, dla których nie jest wykonalna konstrukcja *n*–kąta foremnego. Ile jest takich liczb?

Zad.6.4 Dla jakich naturalnych *n* liczba $\cos\frac{2\pi}{n}$ jest konstruowalna? A $\sin\frac{2\pi}{n}$?

Zad.6.5 Zbadaj, czy są konstruowalne kąty $12°, 3°, 5°, 2°$. Czy jest konstruowalny kąt $75°$? Które spośród kątów $n°$, gdzie $n \in N$, są konstruowalne, a które nie są?