Wszyscy wiemy, że kwadratura koła jest niewykonalna. Nawet w języku potocznym używamy tego terminu na oznaczenie czegoś, co już teoretycznie jest niemożliwe. Na pytanie: czemu kwadratura koła jest niewykonalna, pada przeważnie odpowiedź w rodzaju „a, bo matematycy udowodnili". Tak odpowiadają nawet fachowcy — sądzimy, że ilość matematyków, którzy kiedykolwiek przeczytali dowód niealgebraiczności liczby π (a więc dowód niemożności kwadratury koła) waha się około 1 procenta.

Zamieszczony poniżej artykuł opowiada o tym dowodzie. Właściwie nawet podaje go zupełnie dokładnie. Dowód wykorzystuje kilka pojęć z matematyki tzw. wyższej (funkcje holomorficzne, trochę teorii Galois). Od razu każdy zapyta: czy nie można prościej? Odpowiedź nie jest jednoznaczna. Są, owszem, dowody „bardziej elementarne" — to znaczy nie wykorzystujące aż tylu nowych pojęć i twierdzeń. Czy są to dowody „prostsze", to już rzecz gustu. Czy prościej jest wykopać rów łopatą, czy koparką? I jeszcze jedna myśl. Postęp w matematyce polega nie tylko na przekazywaniu do skarbca wiedzy nowych twierdzeń. Równie ważne jest pokazywanie, jak nowe na ogół bardzo abstrakcyjne teorie stosują się do naszych starych spraw. Elektronika też powinna nam ułatwić życie, a nie tylko umożliwiać rozwój techniki telewizyjnej.

Sto lat dla ludolfiny

Doc. dr Maciej SKWARCZYŃSKI

Niemal dokładnie sto lat temu, w dniu 26 listopada 1882 na uniwersytecie we Fryburgu odbył się wykład Ferdynanda Lindemanna przedstawiający dowód, że $W(\pi) \neq 0$ dla każdego wielomianu

(1) $$W(z) = z^n + c_{n-1}z^{n-1} + \ldots c_1 z + c_0$$

o współczynnikach wymiernych. Tym samym rozstrzygnięty został ostatecznie aktualny od ponad dwóch tysięcy lat problem geometryczny. W jawnej postaci pojawił się on w starożytnej Grecji. Należało wykorzystując jedynie cyrkiel i linijkę skonstruować bok kwadratu, tak aby pole tego kwadratu było równe polu koła o danym promieniu. (W przypadku koła o promieniu 1 należy skonstruować odcinek o długości $\sqrt{\pi}$). Poszukiwana konstrukcja (kwadratura koła) ma nadawać się do teoretycznego uzasadnienia, a więc nie bierzemy pod uwagę rozwiązań wystarczających do zastosowań praktycznych, ale obarczonych błędem. Przykładem takiego przybliżonego rozwiązania jest rezultat Ludolfa van Ceulena z 1610 r, zawierający 32 początkowe cyfry rozwinięcia dziesiętnego liczby π (na jego cześć liczba ta została nazwana ludolfiną). Matematykom starożytnym nie udało się znaleźć kwadratury koła. Dziś, dzięki Lindemannowi, wiemy, że znaleźć jej nie można. W artykule przedstawimy idee, na których opiera się współczesny dowód twierdzenia Lindemanna.

§ 1. Ciała liczbowe

Na początku szesnastego wieku Scipio del Ferro znalazł ogólny wzór wyrażający pierwiastki wielomianu stopnia trzeciego przez współczynniki tego wielomianu. Zwróciło to uwagę matematyków na liczby zespolone i ich arytmetykę. Podjęto również starania, aby znaleźć wzory wyrażające pierwiastki wielomianów wyższych stopni. Badania te doprowadziły do współczesnej teorii ciał (systemów algebraicznych, w których wykonalne są cztery podstawowe operacje arytmetyczne: dodawanie, mnożenie, odejmowanie i dzielenie przez element różny od zera). Bardzo ważnym przykładem jest ciało **Q** wszystkich liczb wymiernych, oraz ciało **C** wszystkich liczb zespolonych. Znaczenie ciała **C** wiąże się z tzw. zasadniczym twierdzeniem algebry, które mówi, że każdy unormowany wielomian $W(z)$ stopnia n o współczynnikach w ciele **C** ma przedstawienie

$$W(z) = (z-a_1)^{m_1}(z-a_2)^{m_2} \ldots (z-a_k)^{m_k},\ m_1 + \ldots + m_k = n,$$

gdzie a_j, $j = 1, 2, \ldots k$, są wszystkimi różnymi zespolonymi pierwiastkami rozpatrywanego wielomianu. Liczba m_j nazywa się krotnością pierwiastka a_j, Nietrudno zauważyć, że $m_j \geqslant 2$ wtedy, gdy $z-a_j$ występuje jako czynnik zarówno w wielomianie $W(z)$, jak też w pochodnej $W'(z)$. Wielomian, który ma wyłącznie pierwiastki jednokrotne, nazywa się wielomianem rozdzielczym.

Liczby zespolone można klasyfikować według własności wielomianów, dla których liczby te są pierwiastkami. Mówimy, że liczba $a \in \mathbf{C}$ jest algebraiczna, jeśli istnieje wielomian o współczynnikach wymiernych, którego a jest pierwiastkiem (twierdzenie Lindemanna powiada, że π nie jest liczbą algebraiczną). Można wykazać, że pierwiastkami wielomianu o współczynnikach algebraicznych są wyłącznie liczby algebraiczne. Zbiór A wszystkich liczb algebraicznych

Ciało liczbowe nazywamy algebraicznie domkniętym, jeżeli każdy wielomian o współczynnikach w tym ciele i nie będący stałą ma w tym ciele pierwiastek. Na przykład ciało liczb rzeczywistych nie jest algebraicznie domknięte, bo wielomian x^2+1 nie ma pierwiastków rzeczywistych. Twierdzenie orzekające, że ciało wszystkich liczb zespolonych jest algebraicznie domknięte, bywa nazywane zasadniczym twierdzeniem algebry.

tworzy ciało, jest ono algebraicznie domknięte. W obecnym artykule będziemy rozpatrywać wyłącznie ciała, które, tak jak ciało **A**, zawierają ciało **Q** liczb wymiernych i zawierają się w ciele **C** liczb zespolonych. Będziemy mówić, że ciało **E** jest rozszerzeniem ciała **F**, jeśli $F \subset E$. Wówczas **E** można rozpatrywać jako przestrzeń wektorową (liniową) nad ciałem **F** (elementy przestrzeni **E** — wektory — można mnożyć przez liczby z ciała **F**). Wymiar tej przestrzeni nazywa się stopniem rozpatrywanego rozszerzenia i jest oznaczany symbolem [**E**: **F**]. Mówimy, że rozszerzenie jest skończone, jeśli jego stopień jest skończony.

Ważnym przykładem jest rozszerzenie pojedyncze $\mathbf{E} = \mathbf{F}(a)$, gdzie a jest ustaloną liczbą algebraiczną. Jest to część wspólna wszystkich ciał zawartych w **C** i zawierających zbiór $F \cup \{a\}$. Ciało to można opisać dokładniej. Ponieważ $F \supset Q$, więc istnieją wielomiany unormowane (tzn. o współczynniku przy najwyższej potędze równym 1) o współczynnikach z F, dla których a jest pierwiastkiem. Można wykazać, że wśród tych wielomianów istnieje dokładnie jeden o najmniejszym stopniu. Nazywa się on wielomianem minimalnym liczby a (nad **F**). Niech Q będzie tym wielomianem; załóżmy, że stopień Q wynosi m. Niech $u_j \in F (j = 0, 1, \ldots, m-1)$ będą współczynnikami tego

wielomianu. Stwierdzamy, że

$$Q(a) = a^m + u_{m-1}a^{m-1} + \ldots u_1 a + u_0 = 0$$

a więc w przestrzeni **E** element a^m jest liniowo zależny od elementów $1, a \ldots, a^{m-1}$. Nietrudno stąd wywnioskować, że elementy $1, a \ldots a^{m-1}$ rozpinają przestrzeń **E**. Są one liniowo niezależne, bo z określenia Q wynika, że a nie jest pierwiastkiem niezerowego wielomianu o współczynnikach w ciele **F** i stopniu mniejszym niż m. Tak więc $[\mathbf{F}(a):\mathbf{F}] = m$ i $\mathbf{F}(a)$ jest rozszerzeniem skończonym.

Podamy przykład ilustrujący wprowadzane pojęcia. Niech $a = \sqrt{3}$. Wtedy ciało $\mathbf{Q}(\sqrt{3})$ składa się z liczb postaci $p+q\sqrt{3}$, gdzie p, q są liczbami wymiernymi. Ponieważ każdą taką liczbę możemy oczywiście przedstawić jako $p\cdot 1+q\cdot\sqrt{3}$, więc wymiar $[\mathbf{Q}(\sqrt{3}):\mathbf{Q}]$ wynosi 2, a bazę stanowią liczby $1, \sqrt{3}$. Podobnie można sprawdzić, że dla $a = \sqrt[3]{2}$, mamy $Q(\sqrt[3]{2}) = \{x: x = p+q\sqrt[3]{2}+r\sqrt[3]{4};\ p, q, r \in \mathbf{Q}\}$, tj. $[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}] = 3$.

Zwróćmy uwagę na pewną własność wielomianu minimalnego liczby a(nad **F**) (skorzystamy z niej później): wielomian ten nie jest rozkładalny nad **F** (tzn. nie jest iloczynem dwu wielomianów niższych stopni dodatnich), bo w przeciwnym przypadku liczba a byłaby pierwiastkiem wielomianu niższego stopnia. Z drugiej strony oba wielomiany $Q(z)$ i $Q'(z)$ mają współczynniki należące do ciała **F** i tę samą własność ma największy wspólny dzielnik tych wielomianów (obliczamy go algorytmem Euklidesa, a więc jego współczynniki należą do ciała zawierającego współczynniki obu wielomianów $Q(z)$ i $Q'(z)$.

Pojęcie pochodnej dla funkcji zmiennej zespolonej jednej zmiennej określamy formalnie takim samym wzorem jak funkcji rzeczywistych

$$f(z_0) = \lim_{z\to z_0} \frac{|f(z)-f(z_0)|}{|z-z_0|}.$$

Dla wielomianów zmiennej zespolonej pochodna wyraża się więc podobnym wzorem, jak dla wielomianów rzeczywistych: $(z^2)' = 2z$, $(z^3)' = 3z^2$, itd.

Ten dzielnik ma stopień niewiększy niż stopień $Q'(z)$, a więc musi być wielomianem stałym, bo wielomian $Q(z)$ nie jest rozkładalny. Zatem $Q(z)$ i $Q'(z)$ nie mają wspólnego czynnika liniowego. W konsekwencji wszystkie zespolone pierwiastki $Q(z)$ są jednokrotne. Jest to zatem wielomian rozdzielczy mający m różnych pierwiastków.

Można udowodnić, że jeśli $\mathbf{F}_1$ jest skończonym rozszerzeniem $\mathbf{F}_0$, oraz $\mathbf{F}_2$ jest skończonym rozszerzeniem $\mathbf{F}_1$, to $\mathbf{F}_2$ jest skończonym rozszerzeniem $\mathbf{F}_0$. Co więcej

$$[\mathbf{F}_2:\mathbf{F}_0] = [\mathbf{F}_2:\mathbf{F}_1][\mathbf{F}_1:\mathbf{F}_0].$$

Wynika stąd, że rozszerzenie $\mathbf{E} = \mathbf{F}(a_1, a_2, \ldots, a_q)$ określone jako część wspólna ciał zawierających zbiór $\mathbf{F} \cup \{a_1, \ldots, a_q\}$ jest skończone. W samej rzeczy, ciało to można otrzymać w wyniku q kolejnych rozszerzeń, z których każde ma stopień skończony.
Mówiąc dokładniej $\mathbf{E} = \mathbf{F}_q$, gdzie

$$\mathbf{F}_1 = \mathbf{F}(a_1),\ \mathbf{F}_2 = \mathbf{F}_1(a_2),\ \ldots,\ \mathbf{F}_q = \mathbf{F}_{q-1}(a_q)$$

§ 2. Metody algebraiczne w geometrii

To, że wychodząc z liczb algebraicznych można skonstruować tylko liczby algebraiczne, można zrozumieć: cyrklem rysujemy tylko okręgi, linijką — proste. Są to zbiory algebraiczne (stopnia 2 i stopnia 1). W przecięciu tych linii pojawić się mogą więc tylko liczby algebraiczne (nie dowolne zresztą).

Istotne znaczenie dla problemu kwadratury koła miała pochodząca od René Descartesa metoda badań oparta o wzajemnie jednoznaczną odpowiedniość między punktami a ich współrzędnymi. Dzieło Descartesa „Géometrie" ogłoszone w 1637 r. jako dodatek do słynnej „Discours de la Méthode" wykazało, że algebra może być przydatnym narzędziem przy analizowaniu problemów geometrycznych. Dzisiaj przy pomocy geometrii analitycznej wykazuje się stosunkowo łatwo, że

wychodząc od punktów płaszczyzny, które mają współrzędne algebraiczne i wykorzystując jedynie cyrkiel i linijkę można w sposób systematyczny konstruować jedynie punkty, których współrzędne są liczbami algebraicznymi. Jeśli kwadratura koła byłaby możliwa, to π jako kwadrat liczby algebraicznej byłaby liczbą algebraiczną, wbrew twierdzeniu Lindemanna. Zatem kwadratura koła nie jest możliwa.

§ 3. Tożsamość Eulera

Długa droga wiodąca do wyjaśnienia natury liczby π zaczyna się od Leonarda Eulera. W książce z 1748 r „Introductio in analysin infinitorum" wykazał on, że funkcja wykładnicza określona w ciele **C** liczb zespolonych związana jest z funkcjami trygonometrycznymi tożsamością

$$e^{x+iy} = e^x(\cos y + i\sin y), \quad x+iy \in C.$$

Dla $x = 0$ i $y = \pi$ otrzymujemy zdumiewająco prostą zależność między liczbą e (podstawa logarytmów naturalnych) a liczbą π

$$e^{i\pi}+1 = 0 \tag{2}$$

(Warto wspomnieć, że współczesne oznaczenie ludolfiny przez grecką literę π pochodzi właśnie od Eulera).

Wzór Eulera bywa nazywany twierdzeniem o pięciu liczbach. Występuje w nim pięć najważniejszych liczb: zero, jeden, e, π oraz i.

Liczby i oraz -1 są algebraiczne. Z równości (2) wynika więc, że twierdzenie Lindemanna jest bezpośrednią konsekwencją nieco mocniejszego rezultatu, znanego jako

Twierdzenie Hermite'a-Lindemanna. *Jeśli liczba zespolona* $a \neq 0$ *jest algebraiczna, to liczba* e^a *nie jest algebraiczna.*
Zobaczymy dalej, że twierdzenie Hermite'a-Lindemanna daje się wykazać przez sprowadzenie do sprzeczności. W tym celu należy zbadać konsekwencje założenia, że obie liczby a oraz e^a są algebraiczne. Jedną z konsekwencji tego założenia jest istnienie skończonego rozszerzenia $\mathbf{Q}(a, e^a)$ ciała **Q**. Należy więc zbadać to rozszerzenie. Przedtem jednak w dwu następnych punktach zajmiemy się ogólnymi własnościami rozszerzeń postaci $\mathbf{F}(a_1, a_2, \ldots, a_q)$ ciała **F**.

§ 4. Twierdzenie Abela o elemencie pierwotnym

Rozszerzenie $\mathbf{F}(a_1, a_2, \ldots, a_q)$ można przedstawić jako rozszerzenie pojedyncze. Ma bowiem miejsce

Twierdzenie Abela. *Jeżeli liczby* $a_1, a_2, \ldots, a_q$ *są algebraiczne, to istnieje liczba algebraiczna* a *taka, że*

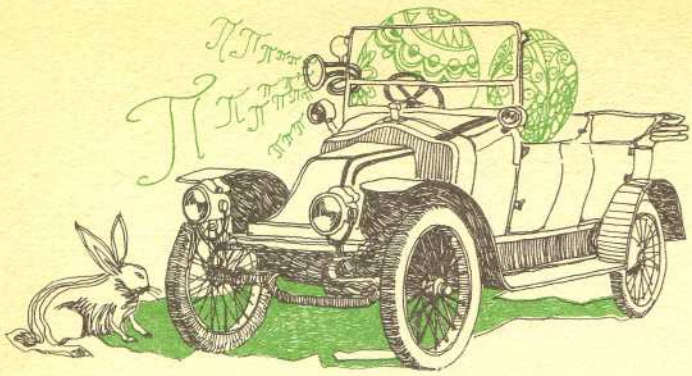
$$\mathbf{F}(a_1, a_2, \ldots, a_q) = \mathbf{F}(a). \tag{3}$$

Liczba a o powyższej własności nazywa się elementem pierwotnym ciała $\mathbf{F}(a_1, a_2, \ldots, a_q)$.

Mamy na przykład $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. Istotnie, mamy $\mathbf{Q}(\sqrt{2}+\sqrt{3}) < \mathbf{Q}(\sqrt{2}, \sqrt{3})$, bo

$$\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})}{2},\quad \sqrt{3} = \frac{(\sqrt{2}+\sqrt{3})^3 - 11(\sqrt{2}+\sqrt{3})}{-2}.$$

Zawieranie przeciwne jest oczywiste.



§ 5. Monomorfizmy i ich przedłużenia

Głębsze wniknięcie w strukturę rozszerzeń skończonych stało się możliwe po roku 1830, kiedy to genialny Ewaryst Galois odkrył, że system algebraiczny można badać analizując różnowartościowe odwzorowania systemu zachowujące działania. Postępowanie to jest analogiczne do badania figury geometrycznej poprzez analizę tych odwzorowań figury, które zachowują odległości między punktami. W naszych rozważaniach podstawową rolę będą odgrywać monomorfizmy ciała $\mathbf{F}$ w ciało $\mathbf{C}$, to znaczy takie różnowartościowe odwzorowania $\mathscr{S}: \mathbf{F} \to \mathbf{C}$, że

$$\mathscr{S}(z_1+z_2) = \mathscr{S}(z_1)+\mathscr{S}(z_2), \quad \mathscr{S}(z_1 z_2) = \mathscr{S}(z_1)\mathscr{S}(z_2).$$

Nietrudno zauważyć, że obraz $\mathscr{S}(\mathbf{F})$ jest ciałem. Tak więc monomorfizm $\mathscr{S}$ ustala wzajemnie jednoznaczną odpowiedniość między ciałami $\mathbf{F}$ i $\mathscr{S}(\mathbf{F})$. Jeśli Q jest wielomianem o współczynnikach w ciele $\mathbf{F}$, to $Q^{\mathscr{S}}$ jest wielomianem, który ma odpowiadające im współczynniki w ciele $\mathscr{S}(\mathbf{F})$. Zauważmy, że $(Q')^{\mathscr{S}} = (Q^{\mathscr{S}})'$. Wynika stąd, że Q jest wielomianem rozdzielczym wtedy, gdy $Q^{\mathscr{S}}$ jest wielomianem rozdzielczym.

Rozpatrzmy rozszerzenie $\mathbf{E}$ ciała $\mathbf{F}$ oraz monomorfizm $\mathscr{S}: \mathbf{F} \to \mathbf{C}$. Monomorfizm $\mathscr{S}^*: \mathbf{E} \to \mathbf{C}$ nazywa się przedłużeniem monomorfizmu $\mathscr{S}$, jeśli $\mathscr{S}^*(z) = \mathscr{S}(z)$ dla każdego $z \in F$. Omówimy przypadek, gdy $\mathbf{E} = \mathbf{F}(a)$.

Lemat 1. *Liczba monomorfizmów $\mathscr{S}^*: \mathbf{E} = \mathbf{F}(a) \to \mathbf{C}$ przedłużających dany monomorfizm $\mathscr{S}: \mathbf{F} \to \mathbf{C}$ jest równa*

$$m = [\mathbf{E}: \mathbf{F}]$$

Dowód. Niech Q będzie wielomianem minimalnym liczby a (nad $\mathbf{F}$). Wielomian Q jest rozdzielczy, a więc również wielomian $Q^{\mathscr{S}}$ jest rozdzielczy. Niech $\mathscr{S}^*$ będzie przedłużeniem monomorfizmu $\mathscr{S}$.
Zauważmy, że przedłużenie to jest całkowicie określone przez wartość $\mathscr{S}^*(a)$ na elemencie a. Z równości

$$\mathscr{S}^*(Q(a)) = Q^{\mathscr{S}}(\mathscr{S}^*(a))$$

i z założenia $Q(a) = 0$ wynika, że $\mathscr{S}^*(a)$ jest pierwiastkiem wielomianu $Q^{\mathscr{S}}$. Wielomian ten jest rozdzielczy, a więc ma m różnych pierwiastków. Istnieje więc co najwyżej m różnych przedłużeń monomorfizmu $\mathscr{S}$.
Z drugiej strony dla każdego pierwiastka a^* wielomianu $Q^{\mathscr{S}}$ istnieje monomorfizm $\mathscr{S}^*$ przedłużający monomorfizm $\mathscr{S}$ i taki, że $\mathscr{S}^*(a) = a$.
Obraz elementu $z = c_{m-1}a^{m-1} + \ldots + c_1 a + c_0 \in F(a)$ jest dany wzorem

$$\mathscr{S}^*(z) = c^*_{m-1}(a^*)^{m-1} + \ldots + c^*_1(a^*) + c^*_0,$$

gdzie $c^*_j = \mathscr{S}(c_j)$ dla $j = 0, 1, \ldots, m-1$.
Tym samym istnieje dokładnie m przedłużeń monomorfizmu $\mathscr{S}$.

Przyjmując w poprzednim lemacie za $\mathbf{F}$ ciało $\mathbf{Q}$ liczb wymiernych, a za $\mathscr{S}$ odwzorowanie tożsamościowe otrzymujemy

Wniosek 1. *Liczba różnych monomorfizmów $\mathscr{S}^*: \mathbf{Q}(a) \to \mathbf{C}$ pozostawiających na miejscu każdą liczbę wymierną jest równa*

$$m = [\mathbf{Q}(a): \mathbf{Q}].$$

Niech $\mathscr{S}_1, \mathscr{S}_2, \ldots, \mathscr{S}_m$ będą tymi monomorfizmami. Dla każdego $u \in Q(a)$ obrazy

$$\mathscr{S}_1(u), \mathscr{S}_2(u), \ldots, \mathscr{S}_m(u)$$

nazywają się liczbami sprzężonymi z u. Jeśli $b \in Q(a)$ jest pierwiastkiem wielomianu nierozkładalnego nad $\mathbf{Q}$, to każdy inny pierwiastek b^* tego wielomianu jest liczbą sprzężoną z b. Rzeczywiście, zgodnie z lematem 1 istnieje monomorfizm $\mathscr{U}: \mathbf{Q}(b) \to \mathbf{C}$ pozostawiający na miejscu każdą liczbę wymierną i taki, że $\mathscr{U}(b) = b^*$. Lemat 1 dla $\mathbf{F} = \mathbf{Q}(b)$, $\mathbf{E} = \mathbf{F}(a_1, a_2, \ldots, a_s) = \mathbf{Q}(a)$ mówi, że monomorfizm $\mathscr{U}$ można przedłużyć na przestrzeń $\mathbf{Q}(a)$ otrzymując monomorfizm $\mathscr{S}_j$, gdzie j jest jedną z liczb $1, 2, \ldots, m$. Oczywiście $\mathscr{S}_j(b) = \mathscr{U}(b) = b^*$, a zatem b^* jest liczbą sprzężoną do b. (Rozpatrzmy dla przykładu cztery monomorfizmy ciała $\mathbf{Q}(\sqrt{2}, \sqrt{3})$. Każdy z nich przeprowadza $\sqrt{2}$ w $\pm\sqrt{2}$ oraz $\sqrt{3}$ w $\pm\sqrt{3}$. Mamy tu cztery możliwości wyboru znaków, po jednej dla każdego monomorfizmu. Wielomian nierozkładalny x^2-2 ma dwa pierwiastki będące liczbami sprzężonymi. Zauważmy, że dwa pierwiastki wielomianu rozkładalnego nie muszą być sprzężone: liczby $\sqrt{2}$ i $\sqrt{3}$ są pierwiastkami wielomianu x^4-5x^2+6, ale nie są sprzężone.)

„Monomorfizm" bywa też nazywany zanurzeniem albo włożeniem. W § 5 wyjaśniony jest więc problem, na ile sposobów $Q(a)$ wkłada się w $\mathbf{C}$ tak, by żadne liczby wymierne „nie ruszyły się". Na przykład gdy $a = \sqrt{2}$, otrzymujemy $[Q(\sqrt{2}): Q] = 2$. Ciało $Q(\sqrt{2})$ można włożyć w $\mathbf{C}$ na dwa sposoby

$$a+b\sqrt{2} \to a+b\sqrt{2}$$

oraz

$$a+b\sqrt{2} \to a-b\sqrt{2}.$$

§ 6. Ślad, norma i rozmiar

Dla każdej liczby $b \in Q(a)$ definiuje się:

1. Ślad liczby b: $\mathrm{Tr}(b) = \sum_{j=1}^{m} \mathscr{S}_j(b)$,

2. Norma liczby b: $\mathrm{N}(b) = \prod_{j=1}^{m} \mathscr{S}_j(b)$,

3. Rozmiar liczby b: $\mathrm{Roz}(b) = \max_{1 \leqslant j \leqslant m} |\mathscr{S}_j(b)|$; znaczenie symboli $\mathscr{S}_1(b), \ldots, \mathscr{S}_m(b)$ jest wyjaśnione przy końcu poprzedniego paragrafu.

§ 6 poświęcony jest głównie dowodowi zdania „Ślad i norma liczby $b \in Q(a)$ są liczbami wymiernymi".

Zauważmy, że $\mathrm{Tr}(b) \in Q$ oraz $\mathrm{N}(b) \in Q$. Rzeczywiście, niech

$$Q(z) = z^k + d_{k-1}z^{k-1} + \ldots + d_1 z + d_0$$

będzie wielomianem minimalnym liczby b (nad $\mathbf{Q}$). Na mocy lematu 1 liczba monomorfizmów ciała $\mathbf{Q}(b)$ pozostawiających na miejscu liczby wymierne jest równa $k = [\mathbf{Q}(b): \mathbf{Q}]$. Oznaczmy te monomorfizmy przez $\mathscr{U}_1, \mathscr{U}_2, \ldots, \mathscr{U}_k$.
Liczby $\mathscr{U}_l(b)$, $l = 1, \ldots, k$, są różnymi pierwiastkami wielomianu $Q(z)$.
Na mocy wzorów Viète'a

$$\sum_{l=1}^{k} \mathscr{U}_l(b) = -d_{k-1} \in Q, \qquad \prod_{l=1}^{k} \mathscr{U}_l(b) = (-1)^k d_0 \in Q.$$

Każdy monomorfizm ciała $\mathbf{Q}(a)$ pozostawiający na miejscu liczby wymierne jest przedłużeniem jednego z monomorfizmów $\mathscr{U}_j$.
Na mocy lematu 1 liczba przedłużeń monomorfizmu $\mathscr{U}_j$ do monomorfizmu ciała $\mathbf{Q}(a)$ jest równa $m/k = [\mathbf{Q}(a):\mathbf{Q}(b)]$ i nie zależy od j.

Wynika stąd, że

$$\mathrm{Tr}(b) = \sum_{j=1}^{m} \mathscr{S}_j(b) = (m/k) \sum_{l=1}^{k} \mathscr{U}_l(b) \in \boldsymbol{Q},$$

$$\mathrm{N}(b) = \prod_{j=1}^{m} \mathscr{S}_j(b) = \Big(\prod_{l=1}^{k} \mathscr{U}_l(b)\Big)^{m/k} \in \boldsymbol{Q}.$$

Tym samym wykazaliśmy, że ślad i norma liczby $b \in \boldsymbol{Q}(a)$ są liczbami wymiernymi. Zauważmy, że odwzorowanie $\mathrm{N}:\boldsymbol{Q}(a) \to \mathbf{Q}$ jest multyplikatywne, oraz $\mathrm{N}(b) = 0$ tylko wtedy, gdy $b = 0$. Odwzorowanie $\mathrm{Tr}: \boldsymbol{Q}(a) \to \mathbf{Q}$ jest addytywne i różnowartościowe, bo $\mathrm{Tr}\,(b) = mb$ dla każdego $b \in \boldsymbol{Q}$. Wnioskujemy stąd, że w przestrzeni liniowej $\boldsymbol{Q}(a)$ nad ciałem $\mathbf{Q}$ odwzorowanie

$$(x, y) \to \mathrm{Tr}(xy)$$

jest niezdegenerowaną (nie równą tożsamościowo zeru) formą dwuliniową. Łatwo teraz wykazać, że dla każdego liniowego odwzorowania $\mathscr{J}: \boldsymbol{Q}(a) \to \mathbf{Q}$ istnieje dokładnie jeden element $y \in \boldsymbol{Q}(a)$ taki, że $\mathscr{J}(x) = \mathrm{Tr}(xy)$ dla wszystkich $x \in \boldsymbol{Q}(a)$. Odwzorowanie $\mathscr{I}: \boldsymbol{Q}(a) \to \mathbf{C}^m$ dane wzorem

$$\mathscr{I}(b) = (\mathscr{S}_1(b), \mathscr{S}_2(b), \ldots, \mathscr{S}_m(b))$$

jest addytywne, liniowe nad $\mathbf{Q}$ i różnowartościowe. (Liniowość wynika stąd, że $\mathscr{S}_j(cb) = \mathscr{S}_j(c)\mathscr{S}_j(b) = c\mathscr{S}_j(b)$ dla każdego $c \in \boldsymbol{Q}$.)

Odwzorowanie $\mathrm{Roz}: \boldsymbol{Q}(a) \to [0, \infty]$ jest dodatnio jednorodne w tym sensie, że dla każdego $c \in \boldsymbol{Q}$

$$\mathrm{Roz}(cb) = |c|\mathrm{Roz}(b).$$

§ 7. Liczby algebraiczne całkowite

Liczby całkowite tworzą zbiór $\boldsymbol{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Liczba wymierna należy do $\boldsymbol{Z}$ wtedy, gdy jest pierwiastkiem jakiegoś unormowanego wielomianu stopnia 1 o współczynnikach w zbiorze $\boldsymbol{Z}$. Fakt ten wskazuje, że pojęcie liczby całkowitej może być uogólnione.
Mówimy, że liczba zespolona jest algebraiczna całkowita, jeśli jest pierwiastkiem jakiegoś unormowanego wielomianu o współczynnikach w zbiorze $\boldsymbol{Z}$. Można wykazać, że wielomian minimalny liczby algebraicznej całkowitej (nad $\mathbf{Q}$) ma współczynniki w zbiorze $\boldsymbol{Z}$.

Suma (a także iloczyn) liczb algebraicznych całkowitych jest liczbą algebraiczną całkowitą. Dla każdej liczby algebraicznej b istnieją liczby dodatnie $c \in \boldsymbol{Z}$ o tej własności, że cb jest liczbą algebraiczną całkowitą. Każda taka liczba c nazywa się mianownikiem liczby b i jest oznaczona symbolem $\mathrm{Mian}\,(b)$. Zbiór wszystkich algebraicznych całkowitych liczb z ciała $\boldsymbol{Q}(a)$ będziemy oznaczać symbolem $\boldsymbol{J}(a)$. Rozpatrzmy dowolną liczbę $b \in \boldsymbol{J}(a)$. Wielomian minimalny liczby b (nad $\mathbf{Q}$) ma współczynniki w zbiorze $\boldsymbol{Z}$, a więc suma i iloczyn pierwiastków tego wielomianu należą do $\boldsymbol{Z}$. Powtarzając rozumowanie z poprzedniego paragrafu przekonujemy się, że $\mathrm{Tr}(b) \in \boldsymbol{Z}$ i $\mathrm{N}(b) \in \boldsymbol{Z}$.

Jak łatwo zauważyć zbiór $\boldsymbol{J}(a)$ jest grupą względem dodawania (mówimy krótko: grupą addytywną). Obrazy $\boldsymbol{Q}(a)$ i $\boldsymbol{J}(a)$ przy odwzorowaniu $\mathscr{I}: \boldsymbol{Q}(a) \to \mathbf{C}^m$ będziemy też oznaczać przez $\boldsymbol{Q}(a)$ i $\boldsymbol{J}(a)$. Stwierdzamy, że $\boldsymbol{J}(a)$ jest addytywną podgrupą w przestrzeni kartezjańskiej $\mathbf{C}^m = \mathbf{R}^{2m}$. Wykażemy, że każdy ograniczony podzbiór $\boldsymbol{K}$ w $\boldsymbol{J}(a)$ jest skończony. Zauważmy, że każdy element $b \in \boldsymbol{J}(a)$ taki, że $\mathscr{I}(b) \in \boldsymbol{K}$ jest pierwiastkiem wielomianu $Q(z)$ unormowanego i minimalnego dla b (nad $\mathbf{Q}$); wystarczy wykazać, że zbiór odpowiednich wielomianów $Q(z)$ jest skończony. Współczynniki wielomianu $Q(z)$ są elementarnymi wielomianami symetrycznymi od pierwiastków tego wielomianu.

Pierwiastki te występują wśród liczb $\mathscr{S}_j(b)$, $j = 1, 2, \ldots, m$, a więc pozostają wspólnie ograniczone, gdy $\mathscr{I}(b)$ przebiega ograniczony zbiór $\boldsymbol{K}$. Zatem każdy ze współczynników wielomianu $Q(z)$ przebiega zbiór ograniczony. Ponieważ współczynniki te są liczbami całkowitymi, więc odpowiednich wielomianów $Q(z)$ jest skończenie wiele. Ma miejsce następujący

Lemat 2. *Jeśli G jest addytywną podgrupą przestrzeni $\mathbf{R}^s$, o tej własności, że każdy ograniczony podzbiór $K \in G$ jest skończony, to istnieją elementy $v_1, v_2, \ldots, v_M \in G$ liniowo niezależne w $\mathbf{R}^s$, takie, że G jest zbiorem kombinacji liniowych postaci*

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_M v_M, \qquad \alpha_j \in \boldsymbol{Z}, j = 1, 2, \ldots, M.$$

Przyjmując $G = \boldsymbol{J}(a)$ i wykorzystując okoliczności, że $\mathscr{I}$ jest izomorfizmem przestrzeni liniowych $\boldsymbol{Q}(a)$ i $\boldsymbol{Q}(a)$ (nad ciałem $\mathbf{Q}$) otrzymuje się następujący

Wniosek 2. *Istnieją takie elementy $v_1, v_2, \ldots, v_M \in \boldsymbol{J}(a)$ liniowo niezależne w przestrzeni $\boldsymbol{Q}(a)$, że $\boldsymbol{J}(a)$ jest zbiorem kombinacji liniowych postaci*

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_M v_M \qquad \alpha_j \in \boldsymbol{Z}, j = 1, 2, \ldots, M.$$

Liczba M jest stopniem rozszerzenia $\boldsymbol{Q}(a)$.

Dowód. Elementy v_j są określone równością $\mathscr{I}(v_j) = v_j$ dla $j = 1, 2, \ldots, M$. Rozpinają one całą przestrzeń $\boldsymbol{Q}(a)$, bo dla każdej liczby $b \in \boldsymbol{Q}(a)$

$$\mathrm{Mian}\,(b) \cdot b \in \boldsymbol{J}(a).$$

Stąd wynika, że jest to baza w $\boldsymbol{Q}(a)$, a więc $M = [\boldsymbol{Q}(a): \mathbf{Q}]$.

Z § 7 najbardziej istotny jest „Wniosek 2", opisujący budowę zbioru liczb algebraicznych całkowitych $\boldsymbol{J}(a)$.

§ 8. Lematy Siegela

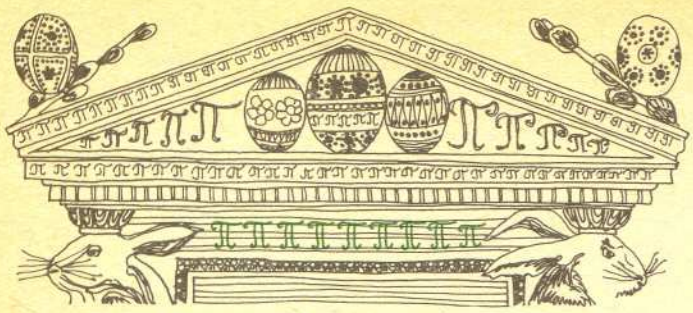
Jeżeli przedmiotów w szufladach jest więcej niż szuflad, to istnieje szuflada zawierająca co najmniej dwa przedmioty. Na tej oczywistej zasadzie „szufladkowej" opiera się dowód lematu Carla Ludwiga Siegela o jednorodnym układzie równań liniowych o współczynnikach całkowitych.

Lemat 3. *Rozpatrzmy k jednorodnych równań liniowych o liczbie niewiadomych $n > k$ i całkowitych współczynnikach b_{ij}*

$$\begin{cases} b_{11}x_1 + \ldots + b_{1n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ b_{k1}x_1 + \ldots + b_{kn}x_n = 0. \end{cases}$$

Załóżmy, że $|b_{ij}| \leqslant B$ dla wszystkich i, j. Wówczas istnieje takie niezerowe rozwiązanie w liczbach całkowitych $x_j \in \boldsymbol{Z}, j = 1, 2, \ldots, n$, że

$$\max_{1 \leqslant j \leqslant n} |x_j| \leqslant 2(nB)^{\frac{k}{n-k}}.$$



Dowód. Rozpatrzmy liniowe odwzorowanie $\mathscr{L}: \mathbf{R}^n \to \mathbf{R}^k$ o macierzy (b_{ij}).
Dla dodatniej liczby całkowitej R połóżmy

$$Z^n(R) = \{x \in Z^n,\ |x_j| \leqslant R,\ j = 1, \ldots, n\}.$$

Zauważmy, że $\mathscr{L}$ odwzorowuje $Z^n(R)$ w $Z^k(nBR)$. Liczba elementów w $Z^n(R)$ jest równa $(2R+1)^n$, a liczba elementów w $Z^k(nBR)$ jest równa $(2nBR+1)^k$. Nierówność $(2R+1)^n > (2nBR+1)^k$ jest spełniona dla dostatecznie dużych R, w szczególności dla

$$R = (nB)^{\frac{k}{n-k}}.$$

Zgodnie z zasadą szufladkową w zbiorze $Z^n(R)$ znajdą się dwa różne elementy mające ten sam obraz przy odwzorowaniu $\mathscr{L}$. Różnica tych elementów $x \in Z^n(2R)$ jest poszukiwanym całkowitoliczbowym rozwiązaniem rozpatrywanego układu równań.

Oznaczmy przez $J(a)$ zbiór liczb algebraicznych całkowitych należących do ciała $\mathbf{Q}(a)$. Nietrudno zauważyć, że zbiór ten jest zamknięty względem dodawania oraz mnożenia. Jak wykazał Siegel, rezultat analogiczny do lematu 3 ma miejsce dla układów równań liniowych o współczynnikach należących do $J(a)$.

Lemat 4. *Rozpatrzmy k jednorodnych równań liniowych o liczbie niewiadomych $n > k$ i współczynnikach $b_{ij} \in J(a)$*

$$\begin{cases} b_{11}z_1 + \ldots + b_{1n}z_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ b_{k1}z_1 + \ldots + b_{kn}z_n = 0 \end{cases}$$

Załóżmy, że $\mathrm{Roz}(b_{ij}) \leqslant B$ dla wszystkich i, j. Wówczas istnieje takie niezerowe rozwiązanie układu $z_j \in J(a)$, $j = 1, \ldots, n$, że

$$\max_{1 \leqslant j \leqslant n} \mathrm{Roz}(z_j) \leqslant C(CnB)^{\frac{k}{n-k}}. \tag{4}$$

(Tu i w dalszym ciągu symbolem C będziemy oznaczać różne stałe zależne jedynie od ciała $\mathbf{Q}(a)$).

§ 9. Algebra funkcji holomorficznych $\mathbf{E}(z, e^z)$

§ 9 poświęcony jest głównie dowodowi technicznego lematu 5.

Rozpatrzmy ciało $\mathbf{E}$ zawarte w $\mathbf{C}$, oraz holomorficzne funkcje $f, g: \mathbf{C} \to \mathbf{C}$. Założenie holomorficzności oznacza istnienie w każdym punkcie $z_0 \in C$ pochodnych zespolonych $Df = f'$ i $Dg = g'$, gdzie

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z)-f(z_0)}{z-z_0},\quad g'(z_0) = \lim_{z \to z_0} \frac{g(z)-g(z_0)}{z-z_0}.$$

Symbolem $E(f, g)$ będziemy oznaczać zbiór złożony z wszystkich funkcji postaci $P(f, g)$, gdzie P jest wielomianem dwóch zmiennych o współczynnikach w ciele $\mathbf{E}$.
Mówimy, że funkcje f i g są algebraicznie niezależne, jeśli z równości $P(f, g) \equiv 0$ wynika, że $P \equiv 0$.
Liczby a i e^a są wartościami w a funkcji holomorficznych z i e^z.

Funkcje te są algebraicznie niezależne, bo jeśli $P \neq 0$, to

$$\lim_{x \to \infty} P(z, e^z) = \infty,\ z = x + iy \in C.$$

Podstawową własnością funkcji wykładniczej jest równość $D(e^z) = e^z$. Operacja różniczkowania D odwzorowuje $\mathbf{E}(z, e^z)$ w siebie. Jeśli $\mathbf{E} = \mathbf{Q}(a, e^a)$, to istnieje nieskończenie wiele takich liczb $w \in C$, że $h(w) \in E$ dla wszystkich $h \in E(z, e^z)$. Liczbami tymi są np. $a, 2a, 3a, \ldots$.
Wykorzystamy następujący

Lemat 5. *Rozpatrzmy liczby algebraiczne $a_1, a_2, \ldots a_q$ oraz rozszerzenie $\mathbf{E} = \mathbf{Q}(a_1, \ldots a_q)$. Niech $f, g: \mathbf{C} \to \mathbf{C}$ będą takimi funkcjami holomorficznymi, że D odwzorowuje $\mathbf{E}(f, g)$ w siebie. Niech $w \in C$ będzie taką liczbą, że $h(w) \in \mathbf{E}$ dla każdego $h \in \mathbf{E}(f, g)$. Wówczas, jeśli $h = P(f, g)$, gdzie P jest wielomianem stopnia r, to dla każdego $p = 0, 1, \ldots$ zachodzi nierówność*

$$\mathrm{Roz}(D^p h(w)) \leqslant \mathrm{Roz}(P)p!r^pC^{p+r} \tag{6}$$

(Tu $\mathrm{Roz}(P)$ oznacza największy rozmiar współczynników wielomianu P).
Ponadto liczby $h(w)$, $Dh(w)$, ..., $D^p h$ (w) mają wspólny mianownik taki, że

$$\mathrm{Mian}(h(w), Dh(w), \ldots, D^p h(w)) \leqslant \mathrm{Mian}\ (P)C^{p+r}. \tag{7}$$

(Tu $\mathrm{Mian}(P)$ oznacza mianownik wspólny dla wszystkich współczynników wielomianu P).

Dowód. Istnieją wielomiany P_j dwu zmiennych, $j = 1, 2$, takie że $Df = P_1(f, g)$, $Dg = P_2(f, g)$. Rozpatrzmy odwzorowanie D_0 algebry wielomianów w siebie określone wzorem

$$D_0 P = (D_1 P)P_1 + (D_2 P)P_2$$

(tu $D_j P$, $j = 1, 2$, oznaczają pochodne cząstkowe).
Sprawdzamy łatwo, że dla każdego P

$$D^p h(w) = D^p P(f(w), g(w)) = (D_0^p P)(f(w), g(w)).$$

Zauważmy, że wielomian P stopnia r spełnia warunek

$$P\mathscr{S}_j < \mathrm{Roz}(P)(1 + z_1 + z_2)^r$$

w tym sensie, że wartość bezwzględna każdego współczynnika wielomianu $P\mathscr{S}_j$ jest niewiększa od odpowiedniego współczynnika wielomianu po prawej stronie.
Ta relacja majoryzowania zachowuje się przy dodawaniu i mnożeniu wielomianów oraz przy obliczaniu pochodnych cząstkowych, a więc zachowuje się przy odwzorowaniu D_0.
Przez indukcję wykazuje się, że

$$D_0^p(P\mathscr{S}_j) < \mathrm{Roz}(P)p!r^pC^p(1 + z_1 + z_2)^{r+p\tau},$$

gdzie τ oznacza większy ze stopni wielomianów P_1 i P_2. Jeśli $Q_1 < Q_2$, to $|Q_1(z_1, z_2)| \leqslant Q_2(|z_1|, |z_2|)$. Stąd wynika, że dla każdego j

$$\left|D_0^p\left(P\mathscr{S}_j\right)\left(\mathscr{S}_j(f(w)), \mathscr{S}_j(g(w))\right)\right| \leqslant \mathrm{Roz}(P)p!r^pC^{p+r}.$$

Dla dowodu żądanej nierówności wystarczy teraz zauważyć, że

$$\begin{aligned} \mathscr{S}_j(D^p h(w)) &= \mathscr{S}_j\left(D_0^p P(f(w), g(w))\right) = \\ &= (D_0^p P)\mathscr{S}_j\left(\mathscr{S}_j(f(w)), \mathscr{S}_j(g(w))\right) = \\ &= D_0^p(P\mathscr{S}_j)\left(\mathscr{S}_j(f(w)), \mathscr{S}_j(g(w))\right). \end{aligned}$$

Oszacowanie mianownika liczby $D^p h(w)$ opiera się na nierówności

$$\mathrm{Mian}(D_0 P) \leqslant \mu\,\mathrm{Mian}(P),$$

gdzie μ jest wspólnym mianownikiem dla wielomianów P_1 i P_2, oraz na prostym rozumowaniu indukcyjnym.

§ 10. Szkic zasadniczej części dowodu

Jeśli obie liczby a i e^a są algebraiczne, to ciało $\mathbf{E} = \mathbf{Q}(a, e^a)$ oraz funkcje $f(z) = z$ i $g(z) = e^z$ spełniają założenia lematu 5.

Wykażemy, że wynika stąd sprzeczność. Zatem założenie, że x jest liczbą algebraiczną, okazuje się fałszywe.

Rozpatrzmy takie punkty $w_1, w_2, \ldots, w_T \in C$, że $h(w_l) \in E$ dla każdego $h \in E(f, g)$ i każdego $l = 1, 2, \ldots T$, gdzie T wybierzemy tak, by $T > 12\,[\mathrm{E}\colon \mathrm{Q}]+12$. Wiemy, że punktów płaszczyzny o powyższej własności jest nieskończenie wiele. To, że za T można przyjąć dowolnie dużą liczbę, ma rozstrzygające znaczenie dla całego dowodu.

Niech r będzie wielokrotnością liczby $2T$ (potem rozpatrzymy granicę przy r dążącym do nieskończoności). Funkcja

$$h = \sum_{i,j=1}^{r} b_{ij} f^i g^j, \quad b_{ij} \in E \tag{8}$$

należy do $E(f, g)$. Niech $n = r^2/(2T)$. Wybierzemy współczynniki b_{ij}, nie wszystkie równe zeru, w taki sposób, aby równość $\mathrm{D}^p h(w_l) = 0$ miała miejsce dla każdego $l = 1, 2, \ldots, T$ i każdego $p = 0, 1, \ldots, n-1$. Problem ten sprowadza się do układu Tn jednorodnych równań liniowych o $r^2 = 2Tn$ niewiadomych b_{ij}. Współczynniki tego układu mają postać $\mathrm{D}^p(f^i g^j)(w_l)$. Zauważmy, że $f^i g^j = P(f, g)$, gdzie P jest jednomianem stopnia niewiększego niż $2r$, oraz $\mathrm{Roz}(P) = 1$. Wykorzystując lemat 5 (nierówności 6 i 7) stwierdzamy, że

$$\mathrm{Roz}(\mathrm{D}^p(f^i g^j)(w_l)) \leqslant p!(2r)^p C^{p+2r} \leqslant n!(2r)^n C^{n+2r} \tag{9}$$

jak również, że wspólny mianownik współczynników układu jest niewiększy niż

$$(C^{n+2r})^T. \tag{10}$$

Mnożąc wszystkie równania układu przez wspólny mianownik współczynników, na mocy nierówności Siegela (4) stwierdzamy, że układ ma niezerowe rozwiązanie w liczbach algebraicznych całkowitych b_{ij} takie, że

$$\mathrm{Roz}(b_{ij}) \leqslant C(Cr^2 n!(2r)^n C^{n+2r})^{\frac{Tn}{2Tn-Tn}}.$$

Ponieważ $n = r\dfrac{r}{2T}$ jest większe od r, oraz $n! \leqslant n^n$, więc

$$\mathrm{Roz}(b_{ij}) \leqslant Cn^{2n} n^n 2^n n^n (C^3)^n \leqslant Cn^{2n}. \tag{11}$$

Funkcje f i g są algebraicznie niezależne, więc $h \neq 0$. Zatem istnieje taka liczba $s \geqslant n$, że $\mathrm{D}^p h(w_l) = 0$ dla $p < s$ i $l = 1, 2, \ldots T$, oraz taka, że $\mathrm{D}^s h(w_l) \neq 0$ dla pewnego l. Bez zmniejszenia ogólności możemy przyjąć, że

$$v = \mathrm{D}^s h(w_1) \neq 0.$$

Oszacujemy $c = \mathrm{Mian}(v)$. Mamy $h = P(f, g)$, gdzie $\mathrm{Mian}(P) = 1$ bo liczby b_{ij} są algebraiczne całkowite. Zatem, na mocy lematu 5 (nierówność (7)), dla dużych s jest

$$c \leqslant C^{2r+s} < s^s.$$

Ten sam lemat daje oszacowanie na rozmiar liczby v. Zauważmy, że P ma stopień $2r$ oraz $\mathrm{Roz}(P) = \max \mathrm{Roz}(b_{ij})$, a więc, wobec (11), nierówność (6) daje dla dużych s

$$\mathrm{Roz}(v) < Cn^{2n} \cdot s!(2r)^s C^{s+2r} < s^{5s}. \tag{12}$$

Niezerowa całkowita liczba $\mathrm{N}(cv)$ jest iloczynem $[\mathrm{E}\colon \mathrm{Q}]$ liczb sprzężonych do cv; jedną z nich jest cv. Z (12) wynika

$$1 \leqslant |\mathrm{N}(cv)| < |cv|(c\,\mathrm{Roz}(v))^{[\mathrm{E}:\mathrm{Q}]-1} < \\ < |v| s^{s[\mathrm{E}:\mathrm{Q}](s5s)([\mathrm{E}:\mathrm{Q}]-1} < |v| s^{6s[\mathrm{E}:\mathrm{Q}]}. \tag{13}$$

Oszacujemy teraz $|v|$ z góry wykazując, że jest to liczba bardzo mała. Skorzystamy w tym celu z zasady maksimum, która mówi, że funkcja holomorficzna w kole domkniętym osiąga największą wartość bezwzględną na brzegu tego koła. Funkcja

$$H(z) = \frac{h(z)}{\prod_{l=1}^{T} (z-w_l)^s}$$

jest holomorficzna w płaszczyźnie C, bo zera mianownika odpowiadają zerom licznika. Jak łatwo zauważyć

$$|v| \leqslant |H(w_1)| s! C^s. \tag{14}$$

Oszacujemy wartość bezwzględną funkcji H na okręgu $|z| = s^{1/2}$ (dla dużych s). Licznik szacujemy z wzoru (8). Wykorzystując (11) i uwzględniając, że $r < (2Ts)^{1/2}$ otrzymujemy dla dużych s

$$|h(z)| \leqslant \mathrm{Roz}(P) \cdot (s^{1/2})^r \cdot (\mathrm{e}s^{1/2})^r < Cs^{2s} s^{s/2} s^{s/2} < s^{4s}.$$

Szacując z dołu mianownik otrzymujemy

$$\prod_{l=1}^{T} |z-w_l|^s \geqslant \prod_{l=1}^{T} (s^{1/2} - |w_l|)^s =$$

$$= s^{Ts/2} \prod_{l=1}^{T} \left[\left(1 - \frac{|w_l|}{s^{1/2}}\right)^{s^{1/2}}\right]^{s^{1/2}} > s^{Ts/2} C^{Ts/2}.$$

Nierówność (14) i zasada maksimum daje dla dużych s oszacowanie

$$|v| < s! C^s |H(w_1)| < s! C^s \frac{s^{4s}}{s^{Ts/2} C^{Ts/2}} < \frac{s^{6s}}{s^{Ts/2} C^{Ts/2}}.$$

Wobec nierówności (13) wynika stąd, że dla dużych s

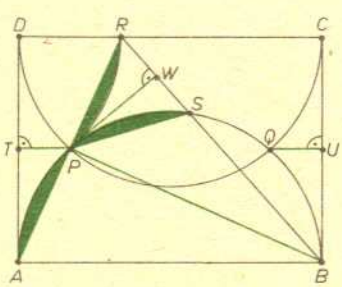
$$1 < |v| s^{6s[\mathrm{E}:\mathrm{Q}]} < \frac{s^{6s([\mathrm{E}:\mathrm{Q}]+1)}}{s^{Ts/2} C^{Ts/2}} = \mathrm{e}^{\left(6[\mathrm{E}:\mathrm{Q}]+6-\frac{T}{2}\right) s \log s - \frac{T}{2} s \log C}$$

W granicy przy r dążącym do nieskończoności s dąży do nieskończoności i prawa strona dąży do zera. Otrzymaliśmy sprzeczność. Tym samym dowód twierdzenia Lindemanna został zakończony.

Literatura

1. S. Lang, *Algebra*, PWN, Warszawa 1975,
2. G. Birkhoff, S. Mac Lane, *Przegląd algebry współczesnej*, PWN, Warszawa 1960,
3. A. Mostowski, M. Stark, *Algebra wyższa*, t. 3, PWN, Warszawa 1954,
4. F. Leja, *Funkcje zespolone*, PWN, Warszawa 1973,
5. D. J. Struik, *Krótki zarys historii matematyki*, PWN, Warszawa 1960,
6. F. Cimpân, *Istoria numaruli π*, Bucuresti 1965 (jest tłumaczenie rosyjskie).

Rozwiązanie zadania M 326.
Kąt APB, jako oparty na średnicy, jest prosty. Ponieważ $AB = BR$, więc punkty APR leżą na jednej prostej i $AP = PR$ oraz $\overline{BP}$ jest dwusieczną kąta ABR. Wobec tego $AP = PR = PS$.
Niech T będzie rzutem prostokątnym P na $\overline{AD}$, U — rzutem Q na $\overline{BC}$, W — rzutem P na $\overline{RS}$. Z przystawania trójkątów APT, RPW i SPW oraz z równości pól „zielonych" mamy a). Wobec $QU = TP = RW = WS$ oraz $TU = TP + PQ + QU = AB = BR = RW + WS + SB$ mamy $PQ = SB$, co daje b).



Rozwiązanie zadania M 325.
Ponieważ kąt wpisany jest równy kątowi dopisanemu opartemu na tym samym łuku (czyli między cięciwą i styczną w jej końcu), gdyż oba są równe połowie kąta środkowego opartego na tymże łuku, więc trójkąty BPQ i DPS, jak też BPR i DPQ są podobne.
Stąd mamy, odpowiednio,

$$\frac{BP}{DP} = \frac{PQ}{PS} \text{ i } \frac{BP}{DP} = \frac{PR}{PQ},$$

czyli $PQ^2 = PR \cdot PS$.