Topologiczny dowód twierdzenia Abela–Ruffiniego

Henryk ŻOŁĄDEK, Warszawa

1. Wstęp

W szkole średniej uczy się młodzież rozwiązywać równania kwadratowe, $x^2 + ax + b = 0$. Wszyscy znamy wzór

$$x = -\frac{a}{2} + \sqrt{\frac{a^2}{4} - b}.$$

Ogólne równanie trzeciego stopnia $x^3 + ax^2 + bx + c = 0$ sprowadzamy najpierw do postaci $y^3 + py + q = 0$ (używając podstawienia $x = y - a/3$). Następne podstawienie $y = z - p/3z$ prowadzi do równania $(z^3)^2 + q(z^3) - p^3/27 = 0$. Stąd dostajemy $z = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}}$, co daje wzór Cardano

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Ogólne równanie stopnia czwartego, które można przyjąć w postaci $x^4 + px^2 + + qx + r = 0$, bada się tzw. metodą Ferrari. Przepisujemy je najpierw w postaci

$$(x^2 + \alpha)^2 - [(2\alpha - p)x^2 - qx + \alpha^2 - r] = 0, \tag{1}$$

gdzie α jest dodatkowym parametrem. Dobieramy α tak aby trójmian kwadratowy w nawiasach kwadratowych był pełnym kwadratem; dokładniej, żądamy aby było

$$q^2 - 4(2\alpha - p)(\alpha^2 - r) = 0. \tag{2}$$

Wtedy równanie (1) sprowadza się do dwóch równań kwadratowych. Z drugiej strony, równanie sześcienne (2) już potrafimy rozwiązać. W ten sposób można rozwiązać wyjściowe równanie czwartego stopnia (chociaż pełny wzór jest na tyle skomplikowany, że nikt nie próbuje go wypisywać).

Udowodniliśmy, że pierwiastki ogólnego równania algebraicznego stopnia ≤ 4 wyrażają się poprzez współczynniki równania za pomocą operacji dodawania, odejmowania, mnożenia, dzielenia i wyciągania pierwiastka naturalnego stopnia. Mówimy, że rozwiązanie równania wyraża się przez *pierwiastniki*. Czasami pierwiastniki są nazywane radykałami.

Przez długi okres matematycy usiłowali znaleźć metodę rozwiązania przez pierwiastniki ogólnego równania piątego stopnia. W 1799 roku P. Ruffini przedstawił dowód nieistniena takiego rozwiązania. Niestety, dowód był zbyt zawiły, aby ówcześni matematycy mogli go zaakceptować. Społeczne przyzwolenie uzyskał dowód analogicznego faktu przeprowadzony w 1824 roku przez N. H. Abela.

Twierdzenie Abela–Ruffiniego. *Ogólne równanie algebraiczne stopnia co najmniej 5 nie daje się rozwiązać przez pierwiastniki. To znaczy, że nie istnieje wzór wyrażający pierwiastki takiego równania przez współczynniki za pomocą operacji algebraicznych i pierwiastków naturalnych stopni.*

Twierdzenie Abela–Ruffiniego stanowiło istotny krok w rozwoju matematyki. Takie pojęcia jak grupa abelowa i grupa rozwiązalna właśnie tutaj biorą swój rodowód.

Później nieco E. Galois zapoczątkował ogólną teorię wiążącą z każdym równaniem algebraicznym pewien niezmiennik, nazwany później grupą Galois. Jest to grupa tych permutacji pierwiastków równania, które zachowują wszystkie relacje algebraiczne zachodzące pomiędzy nimi. Pewne własności równania (np. rozwiązalność przez pierwiastniki) są tłumaczone na własności jej grupy Galois.

Przy takim podejściu główny nacisk przeniesiony został z analitycznych własności rozwiązań (zależność od współczynników) na ich algebraiczny charakter. Zakłada się, że współczynniki należą do zadanego ciała liczbowego

(np. liczb wymiernych) i bada się rozszerzenie tego ciała o pierwiastki równania. Gdy trzeba przyjąć, że współczynniki są zmienne, co jest naturalne przy rozwiązywaniu ogólnych równań, to teoria algebraiczna traci impet. W szczególności, przy dowodzie twierdzenia Abela–Ruffiniego stosowane są dosyć niejasne tricki (rozszerzenia przestępne, algebraiczna niezależność współczynników) po to, aby dostosować się do mocno zakorzenionego schematu algebraicznego.

Poniżej przedstawiamy inny dowód twierdzenia Abela–Rufiniego. Opiera się on na topologicznych własnościach powierzchni Riemanna funkcji algebraicznych, zadanych równaniami algebraicznymi o zmiennych współczynnikach. Czytelnik przekona się, że jest to naturalne i właściwe podejście do problemu.

Niestety żadna książka z teorii liczb i algebry nic nie wspomina o takim dowodzie. Ja pracując nad tym artykułem korzystałem z krótkiej książeczki Aleksejeva [A]. Została ona napisana na podstawie wykładów V. I. Arnolda dla uczniów szkoły–internatu przy Uniwersytecie Moskiewskim przez jednego ze słuchaczy. Przy tym wykładowca musiał zaczynać od zdefiniowana liczb zespolonych, funkcji analitycznych i pojęcia grupy. O istnieniu topologicznego dowodu wspomina się również w monografii Dubrowina, Nowikowa i Fomenki [DNF].

2. Funkcje agebraiczne i ich powierzchnie Riemanna

Naiwne podejście do funkcji algebraicznych może prowadzić do nieporozumień. Na przykład, wiadomo co to jest $\sqrt{x}$ (przyjmuje dwie wartości). Ale ile wartości przyjmuje funkcja $\sqrt{x}+\sqrt{x}$; dwie, cztery, a może trzy? Właściwa definicja jest następująca.

Funkcja algebraiczna to funkcja $y=f(x)$ zadana przez równanie algebraiczne

$$g_n(x)y^n + g_{n-1}(x)y^{n-1} + \ldots + g_0(x) = 0 \tag{3}$$

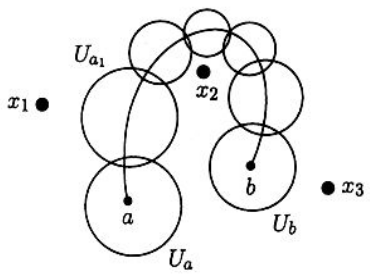
(lub krócej $F(x,y)=0$), gdzie g_j są wielomianami. Dalej dla uproszczenia będziemy zakładać, że $g_n(x)\equiv 1$ (wtedy pierwiastki nie będą uciekać do nieskończoności).

Niech $a\in\mathbb{C}$ będzie takim punktem, że równanie $F(a,y)=0$ ma n różnych pierwiastków $y=z_1,\ldots,z_n$. Wtedy $F'_y(a,z_i)\neq 0$ i z twierdzenia o funkcji uwikłanej wynika, że dla dowolnego x z pewnego otoczenia U_a punktu a równanie $F(x,y)=0$ (względem y) ma także n różnych rozwiązań. Zadają one jednoznaczne funkcje $f_{a,1}(x),\ldots,f_{a,n}(x)$ z dziedziną U_a. Funkcje $f_{a,i}(x)$ rozwijają się w zbieżne szeregi Taylora w punkcie a; zatem za U_a możemy przyjąć dysk (o środku w a) zawarty we wspólnym kole zbieżności tych szeregów.

Pary $(f_{a,i},U_a)$ reprezentują analityczne elementy funkcji f. Ogólny *element analityczny* oznacza się (f_a,U_a), gdzie U_a jest dyskiem o środku w a, w którym jest zbieżny szereg Taylora funkcji f_a w punkcie a.

Element analityczny można przedłużać. Gdyby równanie (3) miało jednoznaczne rozwiązania, to przedłużyłoby się do całej płaszczyzny zespolonej. Na przykład, dla równania $F(x,y)=(y-x)(y-1)$ mamy dwa elementy analityczne, które przedłużają się do funkcji $y=x$ i $y=1$ na $\mathbb{C}$. Przeszkodą w przedłużaniu może okazać się zjawisko sklejania się kilku rozwiązań (lub elementów analitycznych). W powyższym przykładzie mamy sklejenie pozorne w punkcie $x=1$ (bo każde z rozwiązań jest tam przedłużalne w sposób analityczny), ale dla równania $y^3-x=0$ osobliwości w $x=0$ nie da się tak usunąć.

Niech $x_1,\ldots,x_m$ będą punktami osobliwymi funkcji f. Wychodząc z elementu analitycznego (f_a,U_a), $a\in\mathbb{C}\setminus\{x_1,\ldots,x_m\}$, będziemy konstruować powierzchnię Riemanna M funkcji f. Przedłużamy element (f_a,U_a) wzdłuż dróg $\gamma\subset\mathbb{C}\setminus\{x_1,\ldots,x_m\}$ o początku w a (i końcu w b). Pokrywamy γ skończoną

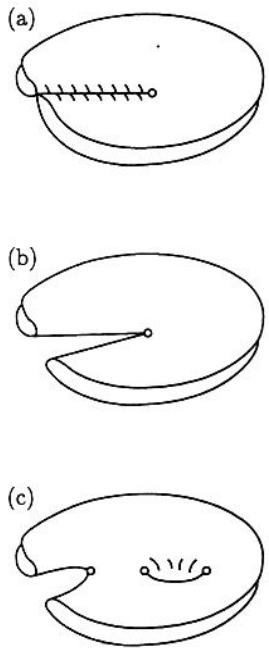


Rys. 1

liczbą otoczeń U_{a_i}, $a_i \in \gamma$, będących dziedzinami elementów analitycznych (f_{a_i}, U_{a_i}) zgodnych na przecięciach, $f_{a_i} \equiv f_{a_{i-1}}$ w $U_{a_i} \cap U_{a_{i-1}}$; przyjmujemy, że $U_{a_0} = U_a$. Końcowy element analityczny (f_b, U_b) jest przedłużeniem elementu analitycznego (f_a, U_a) wzdłuż drogi γ (patrz rysunek 1).

Powstaje pytanie o jednoznaczność przedłużenia analitycznego. Okazuje się, że jeśli dwie drogi $\gamma^{(1)}$ i $\gamma^{(2)}$ (w $\mathbb{C} \setminus \{x_1, \ldots, x_m\}$, o początku w a i końcu w b) dają się zdeformować w sposób ciągły, jedna na drugą, bez ruszania końców i zahaczania o osobliwości, to efekty przedłużeń wzdłuż tych dróg są takie same, $f_b^{(1)} = f_b^{(2)}$. Mówi o tym twierdzenie o monodromii. Łatwo je udowodnić poprzez pokrycie obszaru zakreślonego przez deformowane drogi za pomocą dziedzin U_c elementów analitycznych.

Przedłużając maksymalnie wyjściowy element analityczny (f_a, U_a) dostaje się pewną powierzchnię, którą będziemy nazywać *powierzchnią Riemanna M* funkcji algebraicznej f. Powierzchnia M jest wyposażona w naturalne rzutowanie $\pi : M \to \mathbb{C} \setminus \{x_1, \ldots, x_m\}$ przyporządkowujące wartości $f_c(x)$ (gałęzi f_c) jej argument x.



Rys. 2

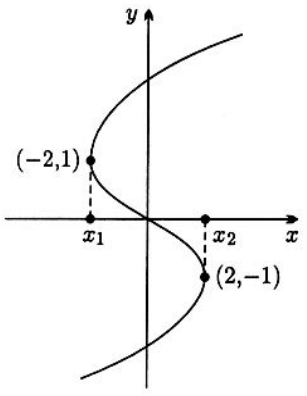
Co prawda, to nie jest jeszcze pełna powierzchnia Riemanna. Dla porządku należałoby ją uzwarcić (w topologii indukowanej przez elementy analityczne) i następnie wygładzić ostrza (cuspy). To dałoby zwartą, gładką i analityczną powierzchnię bez samoprzecięć. Ponieważ nie jest to potrzebne dla celów tego artykułu, pominiemy tę część teorii.

Przykłady. 1. $f(x) = \sqrt{x}$. Powierzchnia Riemanna tej funkcji jest dobrze znana. Startujemy z punktu $a = 1$ i tej gałęzi $f_a(x) = \sqrt{x}$, która jest dodatnia na dodatniej półosi rzeczywistej. Przedłużając tę gałąź wzdłuż okręgu jednostkowego dochodzimy do gałęzi $-f_a(x)$. Aby przedstawić sobie powierzchnię Riemanna tego pierwiastka, bierzemy dwa egzemplarze płaszczyzny $\mathbb{C}$ rozciętej wzdłuż ujemnej półosi rzeczywistej, umieszczone jedna nad drugą i sklejamy krawędzie rozcięcia górnego płata z przeciwległymi krawędziami rozcięcia dolnego płata. Nie można tego przedstawić na płaskim rysunku bez samoprzecięć (rysunek 2(a)). Jednak gdy odwrócimy górny płat, to możemy dokonać sklejeń bez samoprzecięć (rysunek 2(b)). Tak właśnie wygląda powierzchnia Riemanna (nad $\mathbb{C}^* = \mathbb{C} \setminus 0$). Widać, że jest ona homeomorficzna z $\mathbb{C}^*$. Ten homeomorfizm może być zrealizowany analitycznie: $t \to (x, y) = (t^2, t)$, $t \in \mathbb{C}^*$.

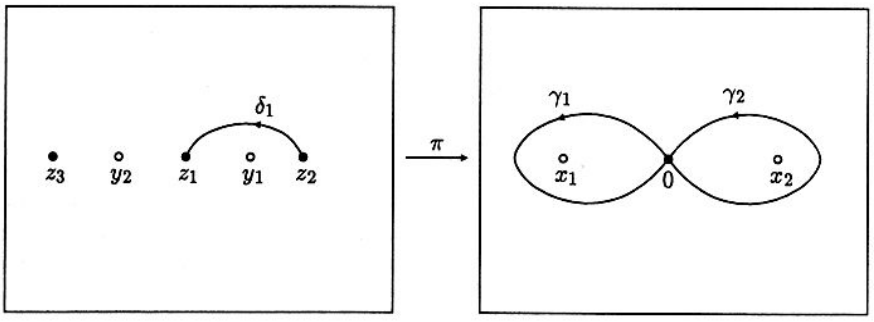
2. $f(x) = \sqrt{x^3 - x}$. Funkcja pod pierwiastkiem ma trzy zera: $0, \pm 1$. Bierzemy dwa egzemplarze płaszczyzny rozciętej wzdłuż odcinków $(-\infty, -1]$ i $[0, 1]$. Odwracamy górny i sklejamy. Można przekonać się, że M jest homeomorficzna z powierzchnią torusa T^2, z którego usunięto 4 punkty. Jeden z usuniętych punktów odpowiada $x = y = \infty$ (rysunek 2(c)).

Czytelnik samodzielnie udowodni, że powierzchnia Riemanna funkcji $\sqrt{x^2 - 1}$ jest homeomorficzna z $\mathbb{C}$ bez dwóch punktów.

3. $y^3 - y = x$. Tutaj powierzchnia Riemanna jest izomorficzna z $\mathbb{C}$ bez dwóch punktów (rysunek 3).



Rys. 3



Ogólna konstrukcja powierzchni Riemanna funkcji algebraicznej $y = f(x)$ zadanej równaniem algebaicznym stopnia n jest następująca. Niech $x_1, \ldots, x_m$ będą punktami osobliwymi. Rozcinamy płaszczyznę za pomocą prostych promieni wychodzących z punktów x_i i biegnących do nieskończoności oraz parami nie przecinających się (można tak zrobić). Bierzemy n egzemplarzy tak rozciętych płaszczyzn. Następnie sklejamy krawędzie rozcięć tak, jak to dyktuje zmiana wartości funkcji $f(x)$ przy obchodzeniu argumentu x wokół punktów osobliwych. Nie zawsze jest to łatwe do wykonania w konkretnych (nietrywialnych) przykładach.

3. Grupa monodromii funkcji algebraicznej

Rozważmy funkcję algebraiczną $y = f(x)$ zadaną równaniem $F(x, y) = y^n + \ldots + g_0(x) = 0$, z punktami osobliwymi $x_1, \ldots, x_m$. Wybierzmy punkt bazowy $a \in \mathbb{C} \setminus \{x_1, \ldots, x_m\}$. Mamy n elementów analitycznych $(f_{a,i}, U_a)$, $i = 1, \ldots, n$ oraz zbiór $M_a = \{z_1, \ldots, z_n\}$ (utożasamiany z $\{1, \ldots, n\}$) wartości funkcji f w a. Grupa monodromii funkcji f jest podgrupą grupy $S(M_a) = S(n)$ permutacji zbioru M_a, definiowaną następująco.

Jeśli γ jest pętlą w $\mathbb{C} \setminus \{x_1, \ldots, x_m\}$ o początku i końcu w a, to przedłużenie analityczne dowolnego elementu $(f_{a,i}, U_a)$ wzdłuż γ prowadzi do nowego elementu, który pokrywa się z jednym z $(f_{a,j}, U_a)$. W szczególności, punkt z_i przechodzi w punkt zbioru M_a, który oznaczymy przez $\Delta_\gamma(z_i)$. Na powierzchni M istnieje droga δ_i o początku w punkcie (a, z_i) i końcu w $(a, \Delta_\gamma(z_i))$, która jest podniesieniem drogi γ do M, oznaczmy to $\pi(\delta_i) = \gamma$. Przekształcenie $\Delta_\gamma : M_a \to M_a$ jest przekształceniem monodromii indukowanym przez pętlę γ. Jest ono wzajemnie jednoznaczne (dlaczego?).

Grupa generowana przez przekształcenia Δ_γ, gdzie γ to pętla, nazywa się *grupą monodromii* i jest oznaczana przez $Mon = Mon(f)$.

Z twierdzenia o monodromii wynika, że przekształcenie Δ_γ jest lokalnie stałe na przestrzeni pętli; nie zmienia się przy deformacji pętli. Klasy równoważności pętli względem deformacji tworzą *grupę fundamentalną* zbioru $\mathbb{C} \setminus \{x_1, \ldots, x_m\}$ z punktem bazowym a, czyli $\pi_1(\mathbb{C} \setminus \{x_1, \ldots, x_m\}, a)$. Operacje grupowe polegają na składaniu dróg i braniu odwrotnej drogi. Mamy więc homomorfizm z $\pi_1(\mathbb{C} \setminus \{x_1, \ldots, x_m\}, a)$ w $S(M_a)$, którego obrazem jest $Mon(f)$.

Przykłady. W powyższych przykładach 1 i 2 mamy $M_a = \{z_1, z_2\}$ i grupa $S(M_a) \simeq \mathbb{Z}/2\mathbb{Z}$ jest generowana przez transpozycję $(1, 2)$. Jeśli pętla γ obiega parzystą liczbę punktów osobliwych (liczoną z krotnościami), to $\Delta_\gamma = id = e$. W przeciwnym przypadku $\Delta_\gamma = (1, 2)$. Zatem $Mon(f) = \mathbb{Z}/2\mathbb{Z}$.

Połóżmy $a = 0$ w Przykładzie 3; wtedy $M_a = \{0, \pm 1\}$. Pętli γ_1 wokół $x_1 = -2$ odpowiada transpozycja wartości $z_1 = 0$ i $z_2 = 1$, tzn. $\Delta_{\gamma_1} = (1, 2)$. Pętli γ_2 wokół $x_2 = 2$ odpowiada transpozycja wartości $z_1 = 0$ i $z_3 = -1$, tzn. $\Delta_{\gamma_2} = (1, 3)$. Stąd nietrudno stwierdzić, że $Mon(f) = S(3)$.

(Zakładamy, że Czytelnik zna zapis permutacji za pomocą rozkładu na cykle. Na przykład, wyrażenie $(142)(36)$ oznacza permutację $1 \to 4, 4 \to 2, 2 \to 1$, $3 \to 6, 6 \to 3, 5 \to 5$ w $S(6)$. Warto jeszcze przypomnieć, że $\sigma \cdot (i_1, \ldots, i_k) \cdot \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$.)

Uwaga 1. Grupę monodromii $Mon = Mon(f)$można utożsamić z grupą Galois pewnego rozszerzenia ciał algebraicznych. Bierzemy jako wyjściowe ciało K ciało $\mathbb{C}(x)$ funkcji wymiernych zmiennej x. Przy tym traktujemy elementy K jako funkcje na U_a . Następnie definiujemy rozszerzenie L jako $K(f_{a,1}, \ldots, f_{a,n})$, dołączenie do funkcji wymiernych gałęzi funkcji algebraicznej. Okazuje się, że grupa automorfizmów rozszerzenia $K \subset L$, tzn. jego grupa Galois $Gal_K L$, pokrywa się z Mon. Rzeczywiście, ponieważ Mon permutuje gałęzie, to indukuje automorfizm ciała L, a ponieważ funkcje z $\mathbb{C}(x)$ są jednoznaczne, są one niezmiennicze względem monodromii. To oznacza, że $Mon \subset Gal_K L$. Załóżmy, że $Mon \neq Gal_K L$. Na podstawie podstawowego twierdzenia teorii Galois (patrz [B]), podgrupie Mon odpowiada ciało pośrednie $K \subset L_1 \subset L$, $L_1 \neq K$ takie, że $Gal_{L_1} L = Mon$ i $L_1 = L^{Mon} = \{\varphi \in L : Mon\, \varphi = \{\varphi\}\}$. Ciało L_1 składa się z tych funkcji, które są niezmiennicze względem monodromii. Są to

zatem funkcje jednoznaczne. Ich osobliwości mają typ co najwyżej potęgowy, również w nieskończoności. Stąd łatwo już wywnioskować (mnożąc przez $(x-x_i)^k$ i stosując twierdzenie Riemanna o usuwaniu osobliwości), że są to funkcje wymierne. To znaczy $L_1 = K$(sprzeczność).

W klasycznych książkach z teorii powierzchni Riemanna, jak np. książka Forstera [F], teoria Galois jest stosowana inaczej. Załóżmy, że powierzchnia Riemanna M jest gładka, zwarta i wyposażona w holomorficzne odwzorowanie $\pi : M \to N = \mathbb{C}P^1$ (przedłużenie rzutowania $(x,y) \to x$), zwane nakryciem rozgałęzionym. To się uzyskuje po dokończeniu konstrukcji z punktu 2. Ciało wyjściowe jest ciałem funkcji wymiernych na N, $K = \mathbb{C}(N)$, które akurat pokrywa się z $\mathbb{C}(x)$. Za to rozszerzenie L jest ciałem funkcji wymiernych na M, przy czym ciało K wkłada się w L za pomocą indukowania $\pi^* : \varphi \to \varphi \circ \pi$. Istotna dla tej teorii jest grupa $Deck = Deck_N M$ automorfizmów nakrycia $M \to N$, złożonych z homeomorfizmów M zachowujących włókna nakrycia. Aby grupa $Deck$ odpowiadała grupie Galois rozszerzenia $K \subset M$ trzeba założyć, że działa ona tranzytywnie na typowym włóknie. Nakrycia spełniające tę własność nazywają się nakryciami Galois. Nakrycia z przykładów 1 i 2 są Galois, ale $Deck$ jest trywialna w przykładzie 3. Nie zauważa się w [F], że klasa takich nakryć jest bardzo wąska w klasie skończonych nakryć rozgałęzionych nad sferą Riemanna. Są to, ni mniej ni więcej, tylko nakrycia zadane przez radykały, $y = w(x)^{p/q}$, gdzie $w(x)$ jest funkcją wymierną.

4. Grupa monodromii typowej funkcji algebraicznej

Pod *typową funkcją algebraiczną* będziemy rozumieć funkcję zadaną równaniem (3), które spełnia następujące warunki:

(i) Zespolona krzywa algebraiczna $\Gamma = \{F(x,y) = 0\} \subset \mathbb{C}^2$ jest gładka i ograniczenie π rzutowania $(x,y) \to x$ do krzywej Γ ma osobliwości najprostszego typu: niezdegenerowane punkty krytyczne z różnymi wartościami krytycznymi.

(ii) Krzywa Γ jest nierozkładalna, tzn. funkcja F nie da się zapisać w postaci iloczynu $F^{(1)}F^{(2)}$ dwu funkcji algebraicznych.

Warunek gładkości oznacza, że (zespolony) gradient funkcji F nie znika: albo $F'_x \neq 0$, albo $F'_y \neq 0$. Punkty krytyczne (x_i, y_i) rzutowania π to takie punkty, w których Γ jest pionowa, tzn. $F'_y = 0$. Ponieważ Γ jest nieosobliwa, to $F'_x \neq 0$ i lokalnie Γ zadaje się równaniem $x - x_i = \psi(y)$, przy czym $\psi(y_i) = \psi'(y_i) = 0$. Warunek niezdegenerowania oznacza, że $\psi''(y_i) = -F''_{yy}/F'_x \neq 0$; tylko dwie gałęzie funkcji algebraicznej zlewają się. Wartości krytyczne rzutowania to x_i; zakłada się, że są one różne.

Przy założeniu (i) powierzchnię Riemanna M można utożsamić z Γ bez punktów krytycznych, punkty zaś osobliwe funkcji algebraicznej są wartościami krytycznymi rzutowania π.

Nierozkładalność zespolonej krzywej algebraicznej Γ gwarantuje jej topologiczną spójność, a tym samym spójność powierzchni Riemanna $M = \Gamma$ bez punktów krytycznych. Rzeczywiście, załóżmy, że Γ nie jest spójna i że zachodzi założenie (i). Wtedy Γ składa się z dwóch rozłącznych krzywych $\Gamma^{(1)}$ i $\Gamma^{(2)}$. Niech $f_i(x)$, $i = 1, \ldots, k$ będą tymi gałęziami (po odpowiednim ponumerowaniu) funkcji $y = f(x)$, które leżą w $\Gamma^{(1)}$, a $f_i(x)$, $i = k+1, \ldots, n$ będą gałęziami drugiej krzywej. Utwórzmy funkcje $F^{(1)}(x,y) = (y - f_1(x))(y - f_2(x)) \ldots (y - f_k(x))$ oraz $F^{(1)}(x,y) = (y - f_{k+1}(x)) \ldots (y - f_n(x))$. Oczywiście mamy $F = F^{(1)}F^{(2)}$. Z drugiej strony, w punktach rozgałęzień krzywe $\Gamma^{(j)}$ są lokalnie spójne i permutacje gałęzi z jednej grupy pozostają w tej samej grupie. To oznacza, że współczynniki (przy potęgach y) wielomianów $F^{(j)}$ są analitycznymi i jednoznacznymi funkcjami, zachowującymi się w nieskończoności jak wielomiany. Zatem są to wielomiany, podobnie jak $F^{(j)}$.

Nierozkładalność można sprawdzić w niektórych przypadkach bezpośrednio. Na przykład, gdy Γ jest obrazem nierozkładalnej krzywej przy algebraicznym odwzorowaniu, to jest nierozkładalna. Jeśli algebraiczne domknięcie Γ w zespolonej płaszczyźnie rzutowej $\mathbb{C}P^2$ jest gładką krzywą, to Γ też jest spójna.

Ostatnia własność oznacza, że część jednorodna najwyższego stopnia wielomianu F rozkłada się na parami różne czynniki liniowe.

Powyższe założenia implikują następujące ważne własności grupy monodromii.

Lemat 1. *Niech funkcja algebraiczna spełnia założenia* (i) *i* (ii). *Wtedy:*
(a) *Mon jest generowana przez transpozycje* (k,l), *odpowiadające zamianom gałęzi* $f_k(x)$, $f_l(x)$ *sklejających się w punkcie krytycznym* (x_i, y_i).
(b) *Mon działa tranzytywnie na zbiorze* $M_a = \{z_1, \ldots, z_n\}$. *To znaczy, że dla każdych dwóch różnych wartości* z_k, z_l *istnieje* $\sigma \in Mon$ *takie, że* $\sigma(z_k) = z_l$.

Dowód. Własność (a) jest oczywista, bo takie transpozycje są indukowane przez pętle wokół x_i. Własność (b) wynika ze spójności Γ. Każde dwa punkty w Γ (tj. (a, z_k) i (a, z_l)) można połączyć (rzeczywistą) krzywą δ. Przy tym można założyć, że rzut $\gamma = \pi(\delta)$ nie przechodzi przez żaden z punktów $x_i = \pi(x_i, y_i)$. γ jest pętlą i $\Delta_\gamma(z_k) = z_l$. Kładziemy $\sigma = \Delta_\gamma$. □

Lemat 2. *Jeśli podgrupa* $G \subset S(n)$ *jest tranzytywna i generowana przez transpozycje, to pokrywa się z* $S(n)$.

Dowód. Powiemy, że podzbiór $A \subset \{1, \ldots, n\}$ jest zupełny, jeśli dowolna permutacja z $S(A)$ przedłuża się do permutacji zbioru $\{1, \ldots, n\}$. Każda transpozycja (k,l) spośród generatorów G definiuje podzbiór zupełny $\{k,l\}$. Niech A_0 będzie maksymalnym podzbiorem zupełnym (względem porządku zawierania). Twierdzimy, że $A_0 = \{1, \ldots, n\}$.

Przypuśćmy, że A_0 jest właściwym podzbiorem. Istnieje transpozycja $\tau = (k,l)$ z $k \in A_0$ i $l \notin A_0$. Wtedy grupa generowana przez $S(A_0)$ i τ byłaby równa $S(A_0 \cup \{l\})$ i zbiór $A_0 \cup \{l\}$ byłby zupełny. □

Wniosek. *Grupa monodromii typowej funkcji algebraicznej jest równa* $S(n)$.

Przykład 4. Grupa monodromii funkcji algebraicznej zadanej równaniem $F = 3y^5 - 25y^3 + 60y - x = 0$ wynosi $S(5)$.

Rzeczywiście, warunek dla punktów krytycznych rzutowania π, $F = F'_y = 15(y^2-4)(y^2-1) = 0$, daje cztery punkty $(x_i, y_i) = \pm(16, 2), \pm(38, 1)$ z różnymi wartościami krytycznymi. W tych punktach krzywa $F = 0$ jest gładka ($F'_x \neq 0$) i rzut jest niezdegenerowany ($F''_{yy} \neq 0$). Z drugiej strony, krzywa $F = 0$ jest obrazem płaszczyzny zespolonej przy algebraicznym odwzorowaniu; (bo x można wyrazić przez y). Zatem są spełnione założenia typowości (i), (ii).

Warto wspomnieć tutaj, że grupa $S(5)$ jest izomorficzna z grupą symetrii dwunastościanu foremnego.

Uwaga 2. W przypadku wielowymiarowym, gdy współczynniki równania algebraicznego zależą od wielu parametrów, mamy do czynienia z wielowymiarowymi powierzchniami Riemanna. Szczególnym przypadkiem jest równanie $y^n + x_{n-1}y^{n-1} + \ldots + x_0 = 0$. Odpowiednia powierzchnia Riemanna jest n-wymiarowa i stanowi n-krotne nakrycie nad uzupełnieniem zbioru wyróżnikowego $\Sigma = \{\Delta(x_0, \ldots, x_{n-1}) = 0\}$. Grupa podstawowa tego uzupełnienia, $\pi_1(\mathbb{C}^n \setminus \Sigma)$, jest tzw. grupą warkoczy $B(n)$, homomorfizm zaś monodromii okazuje się być naturalnym homomorfizmem grupy warkoczy w grupę symetryczną $S(n)$. Oczywiście mamy również $Mon = S(n)$.

5. Grupy rozwiązalne i grupy nierozwiązalne

Komutatorem grupy G jest jej podgrupa $G^{(1)} = [G, G]$ generowana przez elementy $[a,b] = aba^{-1}b^{-1}$, $a, b \in G$. W szczególności, jeśli G jest *abelowa* (tzn. przemienna, $ab = ba$), to $G^{(1)} = \{e\}$. Nietrudno pokazać, że $G^{(1)}$ jest *dzielnikiem normalnym*; tzn. jeśli $a \in G$, $b \in G^{(1)}$, to $aba^{-1} \in G^{(1)}$. Zbiór warstw $G/G^{(1)}$ jest grupą abelową. Określamy indukcyjnie podgrupy (*grupy pochodne*) $G^{(k+1)} = (G^{(k)})^{(1)}$. Mamy zatem ciąg normalnych podgrup (*centralny ciąg pochodny*) $\ldots \subset G^{(2)} \subset G^{(1)} \subset G^{(0)} = G$ z abelowymi grupami ilorazowymi $G^{(k)}/G^{(k+1)}$.

Mówimy, że G jest *rozwiązalna*, jeśli jej centralny ciąg pochodny jest skończony, tzn. $G^{(r)} = \{e\}$ dla pewnego r. Równoważna definicja mówi, że istnieje

skończony ciąg podgrup $\{e\} = G_r \subset G_{r-1} \subset \ldots \subset G_0 = G$ taki, że podgrupy $G_{k+1} \subset G_k$ są dzielnikami normalnymi, a grupy ilorazowe G_k/G_{k+1} są abelowe.

Pojęcie dzielnika normalnego i grupy ilorazowej najwygodniej sobie przedstawić w sytuacji, gdy grupa G działa na pewnym zbiorze A, przy czym pewien podzbiór $B \subset A$ jest niezmienniczy względem tego działania (obrazy elementów z B nie wychodzą poza B). Wtedy zbiór tych przekształceń, które są stałe na B, stanowi podgrupę $H \subset G$. Jest to dzielnik normalny i grupa ilorazowa jest interpretowana jako obcięcie działania G do podzbioru B.

Będziemy korzystali z następującego prostego lematu.

Lemat 3. (a) *Podgrupa grupy rozwiązalnej jest rozwiązalna.*
(b) *Produkt $G \times H$ grup rozwiązalnych jest grupą rozwiązalną.*
(c) *Jeśli grupa H jest rozwiązalna i istnieje surjektywny homomorfizm $G \to H$ z abelowym jądrem, to grupa G jest rozwiązalna.*
(d) *Jeśli G jest rozwiązalna i homomorfizm $G \to H$ jest na, to H jest rozwiązalna.*

Dowód. Tylko punkty (c) i (d) wymagają uzasadnień. W punkcie (c) mamy surjektywny homomorfizm grup pochodnych $G^{(1)} \to H^{(1)}$ z trywialnym jądrem. Zatem $G^{(1)} = H^{(1)}$ i $G^{(r)} = H^{(r)} = \{e\}$ dla pewnego r. W przypadku (d) mamy surjektywne homomorfizmy $G^{(r)} \to H^{(r)}$. □

Przykłady. 5. Grupa $S(2)$ jest abelowa, zatem rozwiązalna.

6. Grupę $S(3)$ można utożsamić z grupą symetrii trójkąta równobocznego (permutacje wierzchołków). Zawiera ona *podgrupę alternującą* $A(3)$ złożoną z permutacji, które rozkładają się na parzystą liczbę transpozycji (czyli odbić trójkąta). Ta ostatnia składa się z obrotów trójkąta, jest dzielnikiem normalnym z dwuelementową grupą ilorazową i jest cykliczna. To daje rozwiązalność $S(3)$.

7. Grupa $S(4)$ ma następujący centralny ciąg pochodny

$$\{e\} \subset V \subset A(4) \subset S(4)$$

gdzie tzw. *Vierergruppe* $V = \{e; (1,2)(3,4); (1,3)(2,4); (1,4)(2,3)\}$. Grupa $S(4)$ jest izomorficzna z grupą obrotów sześcianu (poprzez permutacje diagonal).

Następna własność nie jest tak oczywista jak poprzednie.

Twierdzenie 1. *Grupa $S(n)$, $n \geq 5$, nie jest rozwiązalna.*

Dowód. Powtarzamy go za książką J. Browkina [B]. Ponieważ grupa alternująca $A(n)$ jest dzielnikiem normalnym $S(n)$ z dwuelementową grupą ilorazową, wystarczy dowieść, że $A(n)$ nie jest rozwiązalna. To zaś wynika z następującej obserwacji.

Jeśli cykle $\sigma = (1,2,3)$ i $\tau = (3,4,5)$ (z jednym elementem wspólnym) należą do podgrupy $H \subset A(n)$, to elementy $[\sigma, \tau] = (\sigma(3), \sigma(4), \sigma(5)) \cdot \tau^{-1} =$
$= (1,4,5) \cdot (3,5,4) = (1,4,3)$ oraz $\sigma^{-1}\tau^{-1}\tau\sigma = (\sigma^{-1}(3), \sigma^{-1}(5), \sigma^{-1}(4)) \cdot (3,4,5) =$
$= (2,5,4) \cdot (3,4,5) = (2,5,3)$ należą do komutatora $H^{(1)}$. Te ostatnie też są cyklami z jednym wspólnym elementem.

Powtarzając ten argument, widzimy, że wszystkie pochodne grupy $A(n)^{(j)}$ zawierają dwa cykle z jednym wspólnym elementem. Zatem żadna z nich nie może być trywialna. □

6. Grupy monodromii funkcji wyrażanych przez pierwiastniki

Jeśli $f(x)$ i $g(x)$ są funkcjami algebraicznymi z gałęziami $f_1, \ldots, f_n$, $g_1, \ldots g_k$, to suma $h(x) = f(x) + g(x)$ też jest funkcją algebraiczną. Jej powierzchnia Riemanna jest konstruowana następująco. Bierzemy $n \cdot k$ egzemplarzy płaszczyzny zespolonej, rozciętej wzdłuż promieni idących od wszystkich punktów osobliwych funkcji f i g. Ponumerujemy te płaty za pomocą $h_{i,j}$. Następnie sklejamy brzegi rozcięć posługując się schematem sklejeń dla funkcji f i g; tzn. jeśli przy obieganiu punktu osobliwego płat f_{i_1} przechodzi na płat f_{i_2},

a płat g_{j_1} przchodzi na płat g_{j_2}, to płat h_{i_1,j_1} przechodzi na płat h_{i_2,j_2}. Na koniec należy utożsamić (skleić) te płaty, dla których wartości funkcji $h_{i,j} = f_i + g_j$ pokrywają się. Na przykład, funkcja $y = \sqrt{x} + \sqrt{x}$ ma trzy wartości i spełnia równanie $y(y^2 - 4x) = 0$.

Podobnie definiujemy funkcje algebraiczne i powierzchnie Riemanna dla $f(x) - g(x)$, $f(x) \cdot g(x)$, $f(x)/g(x)$.

Funkcja $h(x) = \sqrt[k]{f(x)}$ składa się z kn gałęzi $h_{j,l}(x) = e^{2\pi ij/k} h_{0,l}(x)$, $j = 0, \ldots, k-1$, $l = 1, \ldots, n$, gdzie $h_{0,l}(x)$ jest wyróżnioną gałęzią pierwiastka $\sqrt[k]{f_l(x)}$. Przy konstruowaniu jej powierzchni Riemanna, oprócz punktów osobliwych wyjściowej funkcji, dochodzą jeszcze punkty rozgałęzienia pierwiastka, czyli zera lub nieskończoności $f_l(x)$. Tak więc bierzemy n paczek po k egzemplarzy rozciętych płaszczyzn. Sklejenia na krawędziach rozcięć są analogiczne jak w przypadku sumy funkcji: jeśli przy obchodzeniu osobliwości f_{l_1} przechodzi na f_{l_2}, to rozcięcia na płatach z l_1–tej paczki są sklejane z rozcięciami płatów l_2–tej paczki, przy czym numery płatów w paczkach ulegają cyklicznemu przesunięciu (trywialnemu, gdy $f_{l_1} \neq 0, \infty$).

Mówimy, że funkcja algebraiczna jednej zmiennej jest przedstawialna przez pierwiastniki, gdy można ją otrzymać z dwóch funkcji 1 i x za pomocą powyższych operacji.

Twierdzenie 2. *Grupa monodromii funkcji algebraicznej przedstawialnej przez pierwiastniki jest rozwiązalna.*

To kończy dowód twierdzenia Abela–Ruffiniego. Wobec tego istnieją równania algebraiczne, które nie dają się rozwiązać za pomocą pierwiastników.

Przykład. Równania $F = 3y^5 - 25y^3 + 60y - x = 0$ (z przykładu 4) nie można rozwiązać przez pierwiastniki.

Dowód twierdzenia 2. Wystarczy pokazać, że jeśli grupy $F = Mon(f)$ i $G = Mon(g)$ są rozwiązalne, to grupy $Mon(f \pm g)$, $Mon(fg)$, $Mon(f/g)$ i $Mon(\sqrt[k]{f})$ też są rozwiązalne. Zajmiemy się tylko przypadkami $f + g$ i $\sqrt[k]{f}$.

Przypomnijmy konstrukcję powierzchni Riemanna funkcji $f + g$. Najpierw wzięliśmy nk egzemplarzy rozciętej płaszczyzny i posklejaliśmy odpowiednio krawędzie rozcięć, a następnie posklejaliśmy całe płaty, na których wartości gałęzi $h_{i,j} = f_i + g_j$ są takie same. Zatem w pierwszym kroku dostaliśmy pewną powierzchnię M', której grupa monodromii jest izomorficzna z pewną podgrupą I grupy $F \times G$. (Może to być podgrupa właściwa, gdy niektóre osobliwości f i g pokrywają się; np. $Mon(\sqrt{x}) = \mathbb{Z}/2\mathbb{Z}$, $Mon(\sqrt[4]{x}) = \mathbb{Z}/4\mathbb{Z}$ ale $Mon(\sqrt{x} + \sqrt[4]{x})$ jest cykliczna rzędu 4).

Przy sklejaniu płatów w drugim kroku niektóre elementy grupy I, te które permutują sklejane płaty, przechodzą w trywialne przekształcenia z grupy monodromii H. Jednakże każdy element z H (indukowany przez pewną pętlę w płaszczyźnie x–ów) jest obrazem pewnego elementu z I, permutacji włókna M'_a indukowanej przez tę samą pętlę. Zatem mamy surjektywny homomorfizm $I \to H$. Teraz wystarczy skorzystać z punktów (a), (b), (d) Lematu 3.

W przypadku funkcji $h = \sqrt[k]{f}$ mamy do czynienia z procesem odwrotnym do sklejania płatów. My powielamy płaty w paczki. Wobec tego mamy surjektywny homomorfizm $H \to G$. Aby móc skorzystać z punktu (c) Lematu 3, musimy pokazać, że jądro tego homomorfizmu jest grupą abelową. Z konstrukcji wynika, że jest ono podgrupą grupy cyklicznej $\mathbb{Z}/k\mathbb{Z}$. □

Literatura

[A] W. B. Alekseew, „Teorema Abela w zadačach i rešeniach", Nauka, Moskwa, 1974 (po rosyjsku).

[B] J. Browkin, „Teoria ciał", PWN, Warszawa, 1978

[DNF] W. A. Dubrowin, S. P. Nowikow i A. T. Fomenko, „Sovremennaja geometria", Nauka, Moskwa, 1986 (po rosyjsku, angielsku, francusku).

[F] O. Forster, „Riemannsche Flächen", Springer–Verlag, Berlin, 1977 (po niemiecku, angielsku).