MATERIAŁY NA XXXIV KONFERENCJĘ Z GEOMETRII ANALITYCZNEJ I ALGEBRAICZNEJ

2013 **Łódź** **str. 27**

FORMUŁA DEDEKINDA

Arkadiusz Płoski (Kielce)

Celem tego opracowania jest dowód formuły Dedekinda pozwalającej obliczyć konduktor pierścienia lokalnego krzywej. W pięknej książce S. S. Abhyankara [1] Czytelnik znajdzie informacje historyczne i przykłady zastosowań konduktora w teorii krzywych algebraicznych. Dla zrozumienia tego wykładu wystarczy znajomość podstawowych faktów z teorii ciał i rozszerzeń całkowitych pierścieni. Materiał ten wykładany jest obecnie w podstawowych kursach algebry takich jak podręcznik S. Langa [2]. Formuła Dedekinda pojawia się w klasycznej monografii O. Zariskiego i P. Samuela [4], w rozdziale poświęconym dziedzinom Dedekinda. Przedstawiona tutaj wersja formuły chociaż oparta na rozumowaniach podanych w [4] jest nieco prostsza i nie wymaga znajomości takich pojęć jak dziedzina Dedekinda i differenta.

Wszystkie rozważane pierścienie są przemienne i mają jedynkę. Pierścienie bez dzielników zera nazywamy dziedzinami. Dziedziną normalną nazywamy dziedzinę całkowicie domkniętą w swoim ciele ułamków. Jeżeli A, B są podzbiorami pewnego pierścienia to symbolem $A \cdot B$ oznaczamy zbiór wszystkich elementów postaci ab gdzie $a \in A$ i $b \in B$.

1 Ślad

Niech L/K będzie skończonym rozszerzeniem ciał stopnia n. Dla każdego elementu $l \in L$ rozważamy odwzorowanie K-liniowe $T_l : L \to L$ dane wzorem $T_l(l') = ll'$ dla

$l' \in L$. Śladem $\mathrm{Tr}_{L/K}$ rozszerzenia L/K nazywamy formę K-liniową $\mathrm{Tr}_{L/K} : L \to L$ zdefiniowaną wzorem $\mathrm{Tr}_{L/K}(l) = \text{ślad } T_l$. Przypomnijmy, że śladem macierzy kwadratowej nazywamy sumę elementów macierzy leżących na głównej przekątnej, ślad T_l = ślad macierzy T_l w ustalonej bazie przestrzeni L/K. Definicja nie zależy od wyboru bazy.

Rozszerzenie L/K nazywamy rozszerzeniem rozdzielczym, gdy $\mathrm{Tr}_{L/K}$ jest formą niezerową. Gdy $n \not\equiv 0 \pmod{\mathrm{char} K}$ (warunek ten jest spełniony gdy $\mathrm{char} K = 0$) to rozszerzenie L/K jest rozdzielcze bo $\mathrm{Tr}_{L/K}(1) = (L : K) = n$.

Dla danego wielomianu $F(y) = y^n + a_1 y^{n-1} + \cdots + a_n \in K[y]$ oznaczamy $F_0(y) = 1$, $F_1(y) = y + a_1$, ..., $F_{n-1}(y) = y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1}$. Zachodzi tożsamość

$$(*) \qquad F(y) - F(z) = (y - z) \sum_{k=0}^{n-1} F_k(z) y^{n-1-k}$$

w pierścieniu $K[y, z]$.

W dalszym ciągu będziemy korzystać z następującej wersji formuły interpolacyjnej Lagrange'a:

Twierdzenie 1.1 *Niech L/K będzie rozszerzeniem rozdzielczym stopnia n i niech $l \in L$ będzie elementem pierwotnym tego rozszerzenia tzn. $L = K(l)$. Jeżeli $F(y) = y^n + a_1 y^{n-1} + \cdots + a_n \in K[y]$ jest wielomianem minimalnym elementu l to dla każdego wielomianu $G(y) \in K[y]$ stopnia $\leqslant n - 1$ mamy:*

$$G(y) = \sum_{k=0}^{n-1} \mathrm{Tr}_{L/K} \left(\frac{G(l)}{F'(l)} F_k(l) \right) y^{n-1-k}.$$

Przed podaniem dowodu twierdzenia przypomnijmy, że

1) jeśli rozszerzenie L/K jest rozdzielcze to każdy wielomian nierozkładalny o współczynnikach w ciele K ma pierwiastki pojedyncze w swoim ciele rozkładu. W szczególności $F'(l) \neq 0$.

2) Jeżeli rozszerzenie $L = K(l)$ jest rozdzielcze i $l_1, \ldots, l_n$ są pierwiastkami wielomianu minimalnego elementu l (zatem $l_i \neq l_j$ dla $i \neq j$ na mocy 1)) to

$$\mathrm{Tr}_{L/K} \left(\frac{H(l)}{G(l)} \right) = \sum_{i=1}^{n} \frac{H(l_i)}{G(l_i)}$$

dla wielomianów $G(y)$, $H(y)$ o ile $G(l_i) \neq 0$ dla $i = 1, \ldots, n$.

Możemy teraz podać
Dowód Twierdzenia 1.1.

Niech $l_1 = l, l_2, \ldots, l_n$ będą pierwiastkami wielomianu $F(y)$ w ciele rozkładu $\bar{L} \supset K$. Na mocy uwagi 1) mamy $F'(l_i) \neq 0$ dla $i = 1, \ldots, n$. Podstawiając w tożsamości (*) pierwiastki l_i na miejsce zmiennej z otrzymujemy

$$\frac{F(y)}{y-l_i} = \sum_{k=0}^{n-1} F_k(l_i) y^{n-1-k}.$$

Formuła Lagrange'a $G(y) = \sum_{i=1}^{n} \frac{G(l_i)}{F'(l_i)} \frac{F(y)}{y-l_i}$ przyjmuje postać

$$\begin{aligned} G(y) &= \sum_{i=1}^{n} \frac{G(l_i)}{F'(l_i)} \sum_{k=0}^{n-1} F_k(l_i) y^{n-1-k} = \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n} \frac{G(l_i)}{F'(l_i)} F_k(l_i) \right) y^{n-1-k} = \\ &= \sum_{k=0}^{n-1} \mathrm{Tr}_{L/K} \left(\frac{G(l)}{F'(l)} F_k(l) \right) y^{n-1-k} \end{aligned}$$

na mocy uwagi 2). □

2 Konduktor

Będziemy rozważać parę dziedzin normalnych R, S spełniających warunki

- S jest rozszerzeniem całkowitym R,
- jeśli L jest ciałem ułamków dziedziny S zaś K ciałem ułamków dziedziny R to rozszerzenie L/K jest rozdzielcze skończonego stopnia n.

Warunki powyższe można opisać następująco: S jest normalizacją dziedziny R w skończonym rozdzielczym rozszerzeniu ciała ułamków R.

Definiujemy

$$\mathrm{compl}(R, S) = \{l \in L : \text{ dla każdego } s \in S \text{ ślad } \mathrm{Tr}_{L/K}(ls) \in R\}.$$

Jest $S \subset \mathrm{compl}(R, S)$ bo ślady elementów S leżą w R. Ponadto $\mathrm{compl}(R, S)$ jest R-podmodułem R-modułu L. Oczywiście $S \cdot \mathrm{compl}(R, S) \subset \mathrm{compl}(R, S)$. Wprowadzone oznaczenie pochodzi od terminu angielskiego “complementary module”.

Niech P będzie podpierścieniem dziedziny S spełniającym warunki

- rozszerzenie S/P jest całkowite,
- S i P mają wspólne ciało ułamków L.

Można też powiedzieć, że S jest normalizacją dziedziny P.

Definiujemy

$$\mathrm{cond}(P, S) = \{l \in L : l \cdot S \subset P\} \quad \text{(konduktor } P\text{)}.$$

Czytelnik sprawdzi, że

- $\mathrm{cond}(P, S) \subset P$ jest ideałem pierścienia P,

- $\mathrm{cond}(P, S)$ jest ideałem pierścienia S,
- jeżeli podzbiór I pierścienia P jest ideałem pierścienia S (a więc także pierścienia P), to $I \subset \mathrm{cond}(P, S)$.

Twierdzenie 2.1 (Formuła Dedekinda) *Niech R będzie dziedziną normalną o ciele ułamków K i niech S będzie domknięciem całkowitym R w skończonym rozszerzeniu rozdzielczym L ciała K. Niech l będzie elementem S takim, że $L = K(l)$ i niech $F(y) = y^n + a_1 y^{n-1} + \cdots + a_n \in K[y]$ będzie wielomianem minimalnym elementu l. Wówczas*

$$\mathrm{cond}(R[l], S) = F'(l) \cdot \mathrm{compl}(R, S).$$

Przed podaniem dowodu powyższego twierdzenia zauważmy, że rozszerzenie S/R spełnia warunki wymienione na początku tego paragrafu. Pierścień $P = R[l]$ jest podpierścieniem dziedziny S o ciele ułamków L. Ponieważ rozszerzenie $S/R[l]$ jest całkowite ($l \in S$!) konduktor $\mathrm{cond}(R[l], S)$ jest poprawnie określony. Wielomian minimalny $F(y)$ ma współczynniki w dziedzinie R.

Dowód Twierdzenia 2.1.

Ustalmy $\tilde{l} \in \mathrm{compl}(R, S)$ i zastosujmy formułę Lagrange'a (Twierdzenie 1.1) do wielomianu $\tilde{l}F'(y)$:

$$\tilde{l}F'(y) = \sum_{k=0}^{n-1} \mathrm{Tr}_{L/K}(\tilde{l}F_k(l))y^{n-k-1}.$$

Współczynniki wielomianów $F_k(y)$ leżą w dziedzinie R. Stąd $F_k(l) \in R[l] \subset S$ a ponieważ $\tilde{l} \in \mathrm{compl}(R, S)$ mamy $\mathrm{Tr}_{L/K}(\tilde{l}F_k(l)) \in R$. Jest zatem $\tilde{l}F'(l) \in R[l]$ a ze względu na dowolność w wyborze $\tilde{l} \in \mathrm{compl}(R, S)$: $F'(l) \cdot \mathrm{compl}(R, S) \subset R[l]$. Ponieważ, jak łatwo sprawdzić, $F'(l)\mathrm{compl}(R, S)$ jest ideałem dziedziny S otrzymujemy $F'(l) \cdot \mathrm{compl}(R, S) \subset \mathrm{cond}(R[l], S)$.

Aby sprawdzić inkluzję w przeciwnym kierunku zauważmy, że $\mathrm{Tr}_{L/K}\left(\frac{s}{F'(l)}\right) \in R$ jeżeli $s \in R[l]$. Rzeczywiście, jeżeli $s \in R[l]$ to $s = G(l)$ dla pewnego wielomianu $G(y)$ stopnia $\leqslant n-1$ i mamy $\mathrm{Tr}_{L/K}\left(\frac{s}{F'(l)}\right) = \mathrm{Tr}_{L/K}\left(\frac{G(l)}{F'(l)}\right) =$ (współczynnik $G(y)$ przy potędze y^{n-1}) $\in R$.

Ustalmy $s_1 \in \mathrm{cond}(R[l], S)$. Wówczas dla każdego $s \in S$ mamy $s_1 s \in R[l]$ bo $s_1 \cdot S \subset \mathrm{cond}(R[l], S)$ a więc $\mathrm{Tr}_{L/K}\left(\frac{s_1 s}{F'(l)}\right) \in R$ na mocy wyżej uczynionej uwagi. Ponieważ $s \in S$ jest dowolne więc $\frac{s_1}{F'(l)} \in \mathrm{compl}(R, S)$ tzn. $s_1 \in F'(l) \cdot \mathrm{compl}(R, S)$. To dowodzi, że $\mathrm{cond}(R[l], S) \subset F'(l) \cdot \mathrm{compl}(R, S)$. $\square$

Wniosek 2.2 *Przy założeniach twierdzenia 2.1:* $\mathrm{cond}(R[l], S) \neq (0)$.

Dowód. Jest $F'(l) \in \mathrm{cond}(R[l], S)$ oraz $F'(l) \neq 0$ bo rozszerzenie L/K jest rozdzielcze. $\square$

Wniosek 2.3 *Załóżmy, że istnieje $l_0 \in S$ takie, że $S = R[l_0]$ i niech $F_0(y) \in R[y]$ będzie wielomianem minimalnym l_0 względem rozszerzenia L/K. Wtedy*

$$\mathrm{compl}(R,S) = \frac{1}{F_0'(l_0)} S.$$

Dowód. Stosujemy formułę Dedekinda do l_0: $\mathrm{cond}(R[l_0], S) = F_0'(l_0) \cdot \mathrm{compl}(R,S)$. Wystarczy zauważyć, że $\mathrm{cond}(R[l_0], S) = \mathrm{cond}(S,S) = S$. □

3 Zastosowanie

Podamy teraz zastosowanie do lokalnej teorii krzywych algebraicznych (por. [3] gdzie podane są podstawowe definicje i twierdzenia). Niech $f = f(x,y) \in \mathbb{K}[[x,y]]$ będzie szeregiem formalnym nierozkładalnym o współczynnikach w ciele algebraicznie domkniętym $\mathbb{K}$. Pierścień $\mathcal{O} = {}^{\mathbb{K}[[x,y]]}/_{(f)}$ nazywamy pierścieniem lokalnym gałęzi $f = 0$. Oznaczmy $\bar{\mathcal{O}}$ domknięcie całkowite dziedziny $\mathcal{O}$ w jej ciele ułamków $\mathcal{M}$. Gałąź $f = 0$ wyznacza waluację $v_f : \mathcal{M} \to \mathbb{Z} \cup \{\infty\}$ ciała $\mathcal{M}$ (por. [3], Uwaga 3.2).

Rozważmy konduktor $\mathcal{C} = \mathrm{cond}(\mathcal{O}, \bar{\mathcal{O}})$ pierścienia lokalnego $\mathcal{O}$ gałęzi $f = 0$ i oznaczmy $c = \dim_{\mathbb{K}} {}^{\bar{\mathcal{O}}}/_{\mathcal{C}}$ (stopień konduktora). Udowodnimy następujące

Twierdzenie 3.1 *Zakładamy, że liczba $n := v_f(x) \neq +\infty$ nie jest podzielna przez* $\mathrm{char}\,\mathbb{K}$. *Wtedy*

$$v_f\left(\frac{\partial f}{\partial y}\right) = c + n - 1.$$

Dowód. Jest $\mathrm{ord}\, f(0,y) = v_f(x) = n \neq +\infty$. Stosując twierdzenie przygotowawcze Weierstrassa stwierdzamy, że można ograniczyć się do przypadku, gdy $f = y^n + a_1(x)y^{n-1} + \cdots + a_n(x) \in \mathbb{K}[[x]][y]$ jest wielomianem wyróżnionym. Ponieważ $n \not\equiv 0 \pmod{\mathrm{char}\,\mathbb{K}}$ zatem na mocy twierdzenia Puiseux (por. [3], Wniosek 2.4) istnieje parametryzacja wierna gałęzi $f = 0$ postaci $(t^n, \psi(t))$. Mamy $\mathcal{O} = \mathbb{K}[[t^n, \psi(t)]]$, $\bar{\mathcal{O}} = \mathbb{K}[[t]]$, $\mathcal{M} = \mathbb{K}((t))$. Czytelnik sprawdzi, że

- $\mathbb{K}[[t]] = \mathbb{K}[[t^n]] + t\mathbb{K}[[t^n]] + \cdots + t^{n-1}\mathbb{K}[[t^n]]$, $\mathbb{K}[[t]]$ jest $\mathbb{K}[[t^n]]$-modułem wolnym rangi n,
- $\mathbb{K}((t)) = \mathbb{K}((t^n))(t)$; rozszerzenie $\mathbb{K}((t))/\mathbb{K}((t^n))$ jest rozdzielcze bo $(\mathbb{K}((t)) : \mathbb{K}((t^n))) = n$ nie dzieli się przez charakterystykę $\mathrm{char}\,\mathbb{K}((t^n)) = \mathrm{char}\,\mathbb{K}$. Wielomianem minimalnym elementu t jest wielomian $f_0(t^n, y) = y^n - t^n$, gdzie $f_0(x,y) = y^n - x$.
- Szereg $\psi(t)$ jest elementem prymitywnym rozszerzenia $\mathbb{K}((t))/\mathbb{K}((t^n))$. Jego wielomianem minimalnym jest wielomian $f(t^n, y) \in \mathbb{K}[[t^n]][y]$.

Do pary pierścieni $R = \mathbb{K}[[t^n]]$, $S = \mathbb{K}[[t]]$ i elementu prymitywnego $\psi(t)$ rozszerzenia $\mathbb{K}((t))/\mathbb{K}((t^n))$ stosuje się Twierdzenie 2.1. Waluacja v_f określona jest wzorem $v_f(g(t^n,\psi(t))) = \operatorname{ord} g(t^n,\psi(t))$. Konduktor $\mathcal{C}$ jest ideałem niezerowym pierścienia $\mathbb{K}[[t]]$ (Wniosek 2.2) a więc $\mathcal{C} = (t^c)\mathbb{K}[[t]]$ dla pewnego c, $c = \dim_{\mathbb{K}} {}^{\mathbb{K}[[t]]}/_{\mathcal{C}}$. Do rozszerzenia $\mathbb{K}[[t]]/\mathbb{K}[[t^n]]$ stosuje się również Wniosek 2.3 (przyjąć $l_0 = t$), który pozwala obliczyć moduł komplementarny $\operatorname{compl}(\mathbb{K}[[t^n]],\mathbb{K}[[t]]) = \frac{1}{t^{n-1}}\mathbb{K}[[t]]$. Z formuły Dedekinda wynika, że $\mathcal{C} = \operatorname{cond}(\mathcal{O},\bar{\mathcal{O}}) = \operatorname{cond}(\mathbb{K}[[t]][\psi(t)],\mathbb{K}[[t]]) = \frac{\partial f}{\partial y}(t^n,\psi(t)) \cdot \left(\frac{1}{t^{n-1}}\mathbb{K}[[t]]\right)$ a stąd $c = \operatorname{ord}\frac{\partial f}{\partial y}(t^n,\psi(t)) - (n-1) = v_f\left(\frac{\partial f}{\partial y}\right) - n + 1$ co dowodzi twierdzenia. $\square$

Literatura

[1] **S. S. Abhyankar**, *Algebraic Geometry for Scientists and Engineers,* AMS, Providance, Rhode Island, 1990.

[2] **S. Lang**, *Algebra,* Addison-Wesley, 1965.

[3] **A. Płoski**, *Wstęp do lokalnej teorii krzywych algebraicznych,* Materiały na XXVIII Konferencję Szkoleniową z Geometrii Analitycznej i Algebraicznej Zespolonej, Łódź 2007, str. 21-40.

[4] **O. Zariski and P. Samuel**, *Comutative algebra, vol. I,* Princeton, D. Van Nostrand, 1958.

THE DEDEKIND FORMULA

Summary. Let R be a normal integral domain with field of fractions K and let $L = K(l)$ be a finite separable algebraic extension of K where l is integral over R. Let S be the integral closure of R in L and let $f(y)$ be the unitary minimal polynomial of l over K. We prove the following version of the Dedekind formula for the conductor $\operatorname{cond}(R[l],S) = \{\tilde{l} \in L : \quad \tilde{l} \cdot S \subset R[l]\}$:

$$\operatorname{cond}(R[l],S) = \frac{\partial f}{\partial y}(l) \cdot \operatorname{compl}(R,S),$$

where $\operatorname{compl}(R,S) = \{\tilde{l} \in L : \forall s \in S \quad \operatorname{Tr}_{L/K}(\tilde{l}s) \in R\}$ is the complementary module of the extension S/R. Then we give an application to plane algebroid branches.

Łódź, 7 – 11 stycznia 2013 r.