Prace Koła Mat. Uniw. Ped. w Krak. 2 (2015), 5-9

Prace Koła Matematyków Uniwersytetu Pedagogicznego w Krakowie (2015)

Kamil Rusek[1]

Lemat Dedekinda–Mertensa[2]

Streszczenie. Z okazji 175. rocznicy urodzin Franciszka Mertensa w artykule przypomniano jeden z Jego rezultatów w dziedzinie algebry, znany współcześnie jako Lemat Dedekinda–Mertensa. Zaprezentowano pochodzący od E. Artina dowód jego klasycznej wersji oraz pewne współczesne uogólnienia i zastosowania.

Abstract. On the occasion of 175^{th} anniversary of the birthday of Franciszek Mertens, in the article one of his result from algebra is recalled, namely that presently known as the Dedekind–Mertens Lemma. The E. Artin proof of its classical version is presented as well as some recent generalizations and applications.

W dniu 20 marca 2015 r. przypadała 175. rocznica urodzin Franciszka Mertensa (zm. 5 marca 1927 r.), wybitnego i wszechstronnego matematyka, profesora Uniwersytetu Jagiellońskiego w latach 1865–1884. Zarys Jego biografii i omówienie wybranych osiągnięć naukowych można znaleźć na przykład w artykule [1].

Studenci matematyki mają szansę zetknąć się z niektórymi rezultatami Mertensa na wykładach z analizy matematycznej (np. twierdzenie o iloczynie szeregów) i z teorii liczb (np. wzór asymptotyczny na funkcję sumacyjną funkcji Eulera φ).

Zapewne mniej znane są dokonania tego uczonego w dziedzinie algebry, którą także się zajmował. Wspomniana rocznica jest więc dobrą okazją do przypomnienia przynajmniej jednego z nich. Wybór autora padł na bardzo ciekawy fakt z algebry przemiennej, udowodniony niemal równocześnie w pracach Dedekinda [3] i Mertensa [10] z 1892 r., zwany w literaturze współczesnej *Lematem Dedekinda–Mertensa*.

Zacznijmy od przypomnienia ważnego pojęcia z algebry przemiennej i postawienia pewnego pytania.

Niech R będzie pierścieniem przemiennym z jedynką a I jego ideałem.

Mówimy, że element $r \in R$ *jest całkowity nad ideałem* I, jeśli

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0$$

AMS (2010) Subject Classification: 13A15, 13B25, 13G05, 13H10.

Słowa kluczowe: domknięcie całkowite ideału, zawartość wielomianu, wielomian Gaussa, liczba Dedekinda–Mertensa.

dla pewnego $n \in \mathbb{N}_+$ oraz pewnych $a_1, \ldots, a_n \in R$, przy czym $a_i \in I^i$ dla $i = 1, \ldots, n$.

Zbiór

$$\overline{I} := \{r \in R \mid r \text{ jest całkowity nad } I\}$$

jest ideałem w R, zwanym *domknięciem całkowitym ideału* I (w R).

Gdy J jest także ideałem pierścienia R, przy czym $I \subset J \subset \overline{I}$, mówimy, że *$J$ jest całkowity nad I*.

Znakomitym źródłem informacji na temat domknięć całkowitych ideałów jest monografia [8].

W badaniach tych domknięć napotykamy następujące pytanie:

Niech R będzie pierścieniem całkowitym oraz I, J jego ideałami. Załóżmy, że I jest całkowity nad pewnym ideałem generowanym przez m elementów, J całkowity nad ideałem generowanym przez n elementów. Czy ideał IJ jest całkowity nad ideałem generowanym przez nie więcej niż $m + n - 1$ elementów?

Pytanie to sprawia wrażenie beznadziejnie trudnego dopóki nie poznamy zapowiedzianego w tytule Lematu Dedekinda–Mertensa. Mając to narzędzie, odpowiedzi można udzielić niemal natychmiast (zob. Wniosek 2).

Nim sformułujemy to twierdzenie, przypomnijmy pewne znane pojęcie z teorii podzielności w pierścieniach wielomianów.

Zawartością wielomianu $f \in R[X]$ nazywamy ideał pierścienia R generowany przez wszystkie współczynniki wielomianu f i oznaczamy symbolem $c(f)$. Jeżeli $c(f) = R$, to wielomian f nazywamy *pierwotnym*.

Wprost z definicji widać, że dla dowolnych $f, g \in R[X]$ mamy inkluzję:

$$c(f)c(g) \supset c(fg). \tag{1}$$

Wiadomo, że w (1) równość zachodzi przy założeniu, że R jest dziedziną ideałów głównych (Lemat Gaussa). Bez tego założenia inkluzja (1) może być ostra, jak pokazuje następujący przykład: dla $f = X + YZ$, $g = Y + XZ \in \mathbb{R}[X, Y][Z]$ mamy $c(f)c(g) = (X, Y)^2 \supsetneq c(fg) = (XY, X^2 + Y^2)$.

Wielomian $g \in R[X]$, dla którego równość $c(fg) = c(f)c(g)$ zachodzi dla każdego $f \in R[X]$, nazywamy *wielomianem Gaussa* (nad R).

Takie wielomiany mają wiele ciekawych własności i są wciąż przedmiotem badań (zob. np. [5], [6]). Przykładem ciekawego wyniku z tej tematyki jest twierdzenie z [5] mówiące, że nad pierścieniem normalnym noetherowskim R zawartość każdego niezerowego wielomianu Gaussa jest *ideałem odwracalnym*, tzn. takim R–podmodułem M ciała ułamków pierścienia R, że $rM \subset R$ dla pewnego $r \in R \setminus \{0\}$ oraz $(R\colon M)M = R$.

Inkluzję (1) można „poprawić" do równości, mnożąc obie strony przez stosowny ideał. Dokładnie o tym mówi tytułowy:

Lemat Dedekinda–Mertensa
Jeżeli $f, g \in R[X]$ oraz $\deg g = n$, to $c(f)^n c(f)c(g) = c(f)^n c(fg)$.

Jak już wspomnieliśmy, Dedekind i Mertens opublikowali nieznacznie różniące się wersje tego twierdzenia w 1892 r. W pracy Dedekinda sformułowanie jest identy-

czne z powyższym, natomiast u Mertensa wykładnik przy $c(f)$ jest postaci $(\deg g)^2$ a na pierścień współczynników nałożone są pewne dodatkowe założenia.

Ten piękny i użyteczny rezultat przez długi czas pozostawał mało znany. Potwierdza to chociażby fakt, że Krull w monografii [9] (z 1968 r.!) formułuje Lemat Dedekinda–Mertensa z wykładnikiem $\deg f + \deg g$.

Trudno też znaleźć w literaturze dowód tego twierdzenia w podanym sformułowaniu (np. w [7] podany jest dość trudny dowód jego znacznie ogólniejszej wersji). Jedyny na jaki autor natrafił, to zamieszczony w pracy Northcotta [11] dowód pochodzący od E. Artina.

Korzystając z tego źródła, przytoczymy tutaj zarys tego pięknego rozumowania.

Dowód Lematu Dedekinda–Mertensa

Dzięki (1) wystarczy pokazać, że $c(f)^n c(f)c(g) \subset c(f)^n c(fg)$. Rozważmy w tym celu pierścień wielomianów $n+1$ zmiennych $R[X, Y_0, \ldots, Y_n]$ i oznaczmy $h := fg$.

Napiszmy (w pełnym pierścieniu ułamków pierścienia $R[X, Y_0, \ldots, Y_n]$) wzór interpolacyjny Lagrange'a:

$$g(X) = \sum_{\nu=0}^{n} g(Y_\nu) \frac{(X - X_0) \cdots (X - Y_{\nu-1})(X - Y_{\nu+1}) \cdots (X - Y_n)}{(Y_\nu - X_0) \cdots (Y_\nu - Y_{\nu-1})(Y_\nu - Y_{\nu+1}) \cdots (Y_\nu - Y_n)}.$$

Mnożąc tę równość stronami przez $f(Y_0) \cdots f(Y_n) \prod_{i \neq j} (Y_i - Y_j)$, otrzymamy

$$f(Y_0) \cdots f(Y_n) g(X) \prod_{i \neq j} (Y_i - Y_j) =$$

$$= \sum_{\nu=0}^{n} h(Y_\nu) f(Y_0) \cdots f(Y_{\nu-1}) f(Y_{\nu+1}) \cdots f(Y_n) W_\nu(X, Y_0, \ldots, Y_n),$$

gdzie $W_\nu \in \mathbb{Z}[X, Y_0, \ldots, Y_n]$ dla $\nu = 0, \ldots, n$.

Korzystając z definicji zawartości wielomianu i wykorzystując całkowitość współczynników wielomianów $\prod_{i \neq j}(Y_i - Y_j), W_0, \ldots, W_n$, łatwo zauważyć, że z ostatniej równości wynika inkluzja

$$c(f)^{n+1} c(g) \subset c(f)^n c(h).$$

■

Wniosek 1

Jeśli R jest pierścieniem całkowitym, $f, g \in R[X]$, to ideał $c(f)c(g)$ jest całkowity nad ideałem $c(fg)$.

Dowód. Dowodzi się (zob. [8, Corollary 1.1.8]), że jeśli I jest ideałem pierścienia całkowitego R, to $r \in R$ jest całkowity nad I wtedy i tylko wtedy, gdy istnieje R–moduł skończenie generowany M, spełniający $rM \subset IM$.

Lemat Dedekinda–Mertensa pozwala zastosować to kryterium do ideału $I := c(fg)$ z R–modułem $M := c(f)^{\deg g}$. ■

Wniosek 1 wraz z pewnymi standardowymi własnościami domknięć całkowitych pozwalają odpowiedzieć twierdząco na pytanie postawione na początku rozważań.

Wniosek 2 ([8, Corollary 1.7.6])
Niech R będzie pierścieniem całkowitym oraz I, J jego ideałami. Załóżmy, że I jest całkowity nad $I' = (a_0, \ldots, a_{m-1})$, J całkowity nad $J' = (b_0, \ldots, b_{n-1})$. Wtedy istnieją takie $c_0, \ldots, c_{m+n-2} \in R$, że ideał IJ jest całkowity nad ideałem $(c_0, \ldots, c_{m+n-2})$.

Dowód. Przyjmijmy $f = a_0 + a_1X + \cdots + a_{m-1}X^{m-1}$, $g = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$. Wtedy $c(f) = I'$, $c(g) = J'$ i na mocy Wniosku 1 ideał $I'J'$ jest całkowity nad ideałem $c(fg) = (c_0, \ldots, c_{m+n-2})$.

Ponieważ ideał IJ jest całkowity nad ideałem $I'J'$, więc również nad ideałem $(c_0, \ldots, c_{m+n-2})$ (zob. [8, Remark 1.3.2]). ■

Wniosek 3 (Lemat Gaussa)
Jeśli R jest pierścieniem całkowitym oraz $f, g \in R[X]$ są pierwotne, to fg jest pierwotny.

Dowód. Ponieważ wielomiany f i g są pierwotne, więc $c(f) = c(g) = R$. Z Wniosku 1 wynika więc, że pierścień R jest całkowity nad swoim ideałem $c(fg)$. Zatem $1 \in c(fg)$. ■

Powiemy teraz o kilku współczesnych uogólnieniach Lematu Dedekinda–Mertensa.

Dla wielomianu $g \in R[X]$ Heinzer i Huneke zdefiniowali w [7] jego *liczbę Dedekinda–Mertensa*:

$$\ell_{DM}(g) := \min\left\{k \in \mathbb{N}_+ : c(f)^{k-1}c(f)c(g) = c(f)^{k-1}c(fg) \text{ dla każdego } f \in R[X]\right\}.$$

Lemat Dedekinda–Mertensa gwarantuje poprawność tej definicji i jest równoważny nierówności:

$$\ell_{DM}(g) \leq 1 + \deg g. \tag{2}$$

W szczególności wynika z niej, że g jest wielomianem Gaussa wtedy i tylko wtedy, gdy $\ell_{DM}(g) = 1$.

Gilmer, Grams i Parker w [4] wzmocnili nierówność (2) następująco:

$$\ell_{DM}(g) \leq \#\{\text{wszytkie niezerowe współczynniki wielomianu } g\}.$$

Nie wdając się w szczegółowe rozważania wspomnijmy tylko, że najdalej idące uogólnienie Lematu Dedekinda–Mertensa podali Heinzer i Huneke w [7] (zob. także [8, Theorem 1.7.3]) dowodząc, że $\ell_{DM}(g) \leq k$, jeśli tylko dla dowolnego ideału maksymalnego $\mathfrak{m}$ pierścienia R ideał $c(g)R_{\mathfrak{m}}$ jest generowany przez k elementów.

Wyjaśnijmy, że $R_{\mathfrak{m}}$ oznacza pierścień ułamków pierścienia R względem zbioru multyplikatywnego $R \setminus \mathfrak{m}$, czyli $R_{\mathfrak{m}} = \{\frac{r}{s} : r \in R, s \notin \mathfrak{m}\}$. Z kolei $c(g)R_{\mathfrak{m}}$ oznacza rozszerzenie ideału $c(g)$ do $R_{\mathfrak{m}}$, czyli ideał w $R_{\mathfrak{m}}$ generowany przez $\imath_{\mathfrak{m}}(c(g))$, gdzie $\imath_{\mathfrak{m}} : R \ni r \longrightarrow \frac{r}{1} \in R_{\mathfrak{m}}$.

Naturalne uogólnienie Lematu Dedekinda–Mertensa na wielomiany wielu zmiennych udowodnił Northcott w [11].

Na zakończenie zwróćmy uwagę na inny kierunek badań, a mianowicie na poszukiwanie odpowiedników Lematu Dedekinda–Mertensa w pierścieniu szeregów formalnych (zob. np. [2]).

Literatura

[1] K. Ciesielski, A. Pelczar, Z. Pogoda, *Franciszek Mertens (1840–1927)*, [w:] *Uniwersytet Jagielloński – Złota Księga Wydziału Matematyki i Fizyki*, Wyd. Naukowe DWN, Kraków, 2000.

[2] N. Epstein, J. Shapiro, *A Dedekind–Mertens theorem for power series rings*, arXiv: 1402.1100v2[math.AC].

[3] R. Fricke, E. Noether, R. Dedekind, Ø. Ore, *Über einen arithmetischen Satz von Gauß* [w:] *Gesammelte mathematische Werke*, MR 237282, JFM 24.0172.01.

[4] R. Gilmer, A. Grams, T. Parker, *Zero divisors in power series rings*, Jour. reine angew. Math. 278/79 (1975), 145–161, MR 0387274, Zbl 0309.13009.

[5] S. Glaz, W. Vasconcelos, *The content of Gaussian polynomials*, J. Algebra 202 (1998), 1–9, MR 1614237, Zbl 0923.13007.

[6] W. Heinzer, C. Huneke, *Gaussian polynomials and content ideals*, Proc. Amer. Math. Soc. 125 (1997), 739–745, MR 1401742, Zbl 0860.13005.

[7] W. Heinzer, C. Huneke, *The Dedekind–Mertens Lemma and the contents of polynomials*, Proc. Amer. Math. Soc. 126 (1998), 1305–1309, MR 1425124, Zbl 0903.13001.

[8] C. Huneke, I. Swanson, *Integral Closure of Ideals, Rings, and Modules*, Cambridge Univ. Press, Cambridge, 2006, MR 2266432, Zbl 1117.13001.

[9] W. Krull, *Idealtheorie*, Zweite, ergänzte Auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 46, Springer-Verlag, Berlin-New York, 1968 (German). MR 0229623, Zbl 0155.36401.

[10] F. Mertens, *Über einen algebraischen Satz*, S. B. Akad. Wiss. Wien, Math.-nautw. Kl.., Abt. IIa 101 (1892), 1560–1566, JFM 24.0085.05.

[11] D. G. Northcott, *A generalization of a theorem on the content of polynomials*, Proc. Cambridge Philos. Soc. 55 (1959), 282–288, MR 0110732, Zbl 0103.27102.

[1] *Instytut Matematyki*
Uniwersytet Pedagogiczny w Krakowie
ul. Podchorążych 2, 30-084 Kraków
E-mail: krusek@up.krakow.pl

Przysłano: 5.05.2015; publikacja on-line: 7.07.2015.

[2] jest to nieco rozszerzona wersja referatu wygłoszonego przez autora na X. Ogólnopolskim Sympozjum Kół Naukowych „Odkryj piękno matematyki” w dniu 20 marca 2015 r..