ALGEBRA, LOGIC AND NUMBER THEORY
BANACH CENTER PUBLICATIONS, VOLUME 108
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2016

SOME REMARKS ABOUT THE DEDEKIND–MERTENS LEMMA

JAKUB BYSZEWSKI

Institute of Mathematics, Jagiellonian University
Łojasiewicza 6, 30-348 Kraków, Poland
E-mail: jakub.byszewski@uj.edu.pl

Abstract. The Dedekind–Mertens lemma relates the contents of two polynomials and the content of their product. Recently, Epstein and Shapiro extended this lemma to the case of power series. We review the problem with a special emphasis on the case of power series, give an answer to a question posed by Epstein–Shapiro and investigate extensions of some related results. This note is of expository character and discusses the history of the problem, some examples and announces some new results.

1. Introduction. One of the classical forms of the Gauss lemma says that a product of two primitive polynomials with integer coefficients is primitive. Here, a polynomial is primitive if the greatest common divisor of its coefficients is one. In fact, such a statement can be phrased so as to hold over an arbitrary ring of coefficients R. In this note, all rings are considered commutative and with unity. In fact, redefine a polynomial $f \in R[X]$ or a power series $f \in R[\![X]\!]$ to be primitive if its coefficients generate the trivial ideal. Then the product of two primitive polynomials is primitive. The proof is trivial: If $f, g \in R[X]$ were primitive polynomials, but fg were not, there would exist a maximal ideal $\mathfrak{m}$ containing all the coefficients of fg. We immediately get a contradiction by reducing modulo $\mathfrak{m}$ (since in the ring $R/\mathfrak{m}[X]$ a product of two nonzero elements is nonzero). Note that the same proof shows that the statement remains true if we consider a product of two primitive *power series*.

However, there is another way to generalize the statement of the Gauss lemma to arbitrary rings. For a polynomial or a power series f with coefficients in the ring R, we define the content ideal $c(f)$ to be the ideal of R generated by the coefficients of f. Another way to phrase the Gauss lemma is to say that whenever f and g are polynomials with

2010 *Mathematics Subject Classification*: Primary: 13F25, 13A15; Secondary: 13B25.
Key words and phrases: Dedekind–Mertens lemma, content of a power series.
The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc108-0-3

integer coefficients, then $c(fg) = c(f)c(g)$ holds. Such a statement does not generalize literally to arbitrary rings.

EXAMPLE 1.1. Let $R = k[s,t]$, $f, g \in R[X]$, $f = s - tX, g = s + tX$. Then $fg = s^2 - t^2X^2$ and the content ideals are $c(f) = c(g) = (s,t)$ and $c(fg) = (s^2, t^2) \neq (s,t)^2 = c(f)c(g)$.

In general the equality $c(fg) = c(f)c(g)$ is quite close to being true, however. First of all, the inclusion $c(fg) \subseteq c(f)c(g)$ is trivial. Further, these two ideals have the same radicals. In fact, passing to the quotient ring $R/\mathfrak{p}$, and considering the images $\bar{f}, \bar{g} \in R/\mathfrak{p}[X]$ of the polynomials f and g, we immediately see that the ideals $c(fg)$ and $c(f)c(g)$ are contained in precisely the same prime ideals $\mathfrak{p}$, and hence $\operatorname{rad} c(f)c(g) = \operatorname{rad} c(fg)$.

However, in the case of Example 1.1, a more subtle equality holds. We have $c(f)^2c(g) = c(f)c(fg)$ (in this case both sides are equal to the ideal $(s,t)^3$). In fact, a similar equality always holds: there always exists an integer $k \geq 1$ such that $c(f)^k c(g) = c(f)^{k-1}c(fg)$. This result was discovered by Dedekind [D] and Mertens [M] (independently) in 1892 for polynomials whose coefficients are algebraic integers, but follows also from an earlier result of Kronecker [K]. In fact, the result of Dedekind stated in a modern language is as follows.

THEOREM 1.2 (Dedekind–Mertens, 1892). *Let R be a ring and $f, g \in R[X]$. Then*

$$c(f)^k c(g) = c(f)^{k-1}c(fg),$$

where $k = 1 + \deg(g)$.

The proof of this result is strictly combinatorial. In fact, a stronger statement holds, namely $c_{\mathbf{Z}}(f)^k c_{\mathbf{Z}}(g) = c_{\mathbf{Z}}(f)^{k-1}c_{\mathbf{Z}}(fg)$, where $c_{\mathbf{Z}}(f)$ denotes the abelian group generated by the coefficients of f.

This statement has been improved in 1998 by Heinzer–Huneke [HH], who proved that one can replace the constant k in the statement of the Dedekind–Mertens lemma by the minimal local number of generators of the ideal $c(g)$. For an ideal I, denote by $\mu(I)$ the minimal number of generators of I.

THEOREM 1.3 (Heinzer–Huneke, 1998). *Let R be a ring and $f, g \in R[X]$, $g \neq 0$. Then*

$$c(f)^k c(g) = c(f)^{k-1}c(fg),$$

where $k = \max_{\mathfrak{m}} \mu(c(g)R_{\mathfrak{m}})$, the maximum being taken over all maximal ideals $\mathfrak{m}$ of R.

There is a considerable difference between the statement of Dedekind–Mertens and the improvement due to Heinzer–Huneke. In the former case, the statement is combinatorial, and one can in fact produce universal polynomials expressing the left hand side in terms of the natural generators of the right hand side. This is not the case for Heinzer–Huneke, as this statement clearly depends on the choice of the ring R.

2. Dedekind–Mertens lemma for power series. It is natural to ask whether the Dedekind–Mertens lemma can be generalized to power series rings, i.e., whether for power series $f, g \in R[\![X]\!]$, the equality $c(f)^k c(g) = c(f)^{k-1}c(fg)$ holds for some integer $k \geq 1$. The first example that this is not the case was given in 1978 by David E. Rush [R]. In his example, the ring of coefficients is $R = k[s,t]$, the ring of polynomials in two

variables. However, in 2014 Neil Epstein and Jay Shapiro [ES] revisited the example of Rush, discovered that it is wrong, and managed, in fact, to prove that no such example exists when the ring R is noetherian. We first state the example of Rush, discuss why it is incorrect, and then state the result of Epstein and Shapiro.

EXAMPLE 2.1. Let $R = k[s,t]$, and consider the following power series

$$f = s + X,\ g = t + \frac{sX}{1-X}\,.$$

Then

$$fg = st + tX + \frac{s(s+X)X}{1-X} = st + (t+s^2)X + (s+s^2)X^2 + (s+s^2)X^3 + \dots$$

and $c(f) = R$, $c(g) = (t,s)$, $c(fg) = (st, t+s^2, s+s^2)$. Rush claimed that $c(g) \neq c(fg)$. However, this is not the case and in fact $c(fg) = c(g)$. Indeed, $s = (1-s)(s+s^2) + s(t+s^2) - st$ and $t = (1+s)(t+s^2) - s(s+s^2) - st$ are both in $c(fg)$.

In fact, the result of Epstein and Shapiro says that the theorem of Heinzer–Huneke generalizes without any trouble to the case of power series over a *noetherian* ring.

THEOREM 2.2 (Epstein–Shapiro, 2014). *Let R be a noetherian ring, $f, g \in R[\![X]\!]$. Let*

$$k = \max_{\mathfrak{m}} \mu(c(g)R_{\mathfrak{m}}).$$

Then

$$c(f)^k c(g) = c(f)^{k-1} c(fg).$$

In their article, Epstein and Shapiro discuss also the question whether the assumption that R is noetherian can be relaxed. They first note ([ES], Example 4.1) that the exponent k cannot be improved when f and g are generic polynomials. This follows from a result of [CVV], Theorem 1. More precisely, if $f = \sum_{i=0}^{n} s_i X^i$, $g = \sum_{i=0}^{n} t_i X^i$ are polynomials with coefficients in the ring of polynomials $R = \mathbf{Z}[s_0, s_1, \dots, s_n, t_0, t_1, \dots, t_n]$, then the equality $c(f)^k c(g) = c(f)^{k-1} c(fg)$ holds if and only if $k \geq n+1$. It follows that if we take $f = \sum_{i=0}^{\infty} s_i X^i$, $g = \sum_{i=0}^{\infty} t_i X^i$ to be power series with algebraically independent coefficients, the equality $c(f)^k c(g) = c(f)^{k-1} c(fg)$ fails for any integer k. (To see that, substitute $s_i = t_i = 0$ for $i \geq k+1$.)

It is clear that the claim of the Dedekind–Mertens lemma fails here because the ideal $c(g)$ is infinitely generated, and the value of k produced by the Epstein–Shapiro theorem is infinite. In the article [ES], the authors ask whether this is perhaps the only obstruction for the Dedekind–Mertens lemma to hold. More precisely, they ask the following question:

QUESTION 2.3 ([ES], section 4). *Let R be a ring, $f, g \in R[\![X]\!]$. Let $k = \max_{\mathfrak{m}} \mu(c(g)R_{\mathfrak{m}})$. Suppose that $k < \infty$. Then does the equation $c(f)^k c(g) = c(f)^{k-1} c(fg)$ hold?*

We will show that the answer to this question is negative. In fact, the first example of such a phenomenon is already implicitly contained in the work of D. Fields from 1971.

EXAMPLE 2.4. In [F], the following example is constructed in order to show that power series with invertible content can be zero divisors. Let S be a ring and let

$$R = S[Z, Y_0, Y_1, Y_2, \dots]/I,$$

where I is the ideal generated by Y_0Z and $Y_i - Y_{i+1}Z$, $i \geq 0$. Denote by z and y_i the classes of Z and Y_i in R and let

$$f = \sum_{i\geq 0} y_i X^i, \quad g = z - X$$

be power series in $R[\![X]\!]$. Then $c(g) = R$ and $c(f) = (y_0, y_1, \ldots) \neq 0$, but $fg = 0$ and $c(fg) = 0$. The value of $k = \max_{\mathfrak{m}} \mu(c(g)R_{\mathfrak{m}}) = 1$, but the equality $c(f)^k c(g) = c(f)^{k-1}c(fg)$ fails. In particular, the polynomial g is a zero divisor in the ring of power series $R[\![X]\!]$. Note that the ring R is not noetherian. In fact, if R was noetherian, the formula in the Dedekind–Mertens lemma would hold for $k = 1$. Furthermore, note that if we invert the role of f and g, the equality $c(g)^k c(f) = c(g)^{k-1}c(fg)$ fails for any value of $k \geq 1$. This is related to the fact that the ideal $c(f)$ is not finitely generated.

Example 2.5. We give a modified version of Fields's example below. We believe that it makes it easier to follow what is happening. Let R be a valuation ring with valuation group $\mathbf{Z}^2$ (with respect to the lexicographic ordering). Let a be an element of valuation $(0,1)$ (so that a generates the maximal ideal $\mathfrak{m}$ of R) and let b be an element of valuation $(1,0)$. The ring R has precisely three prime ideals, namely 0, $\mathfrak{m}$ and

$$\mathfrak{n} = \{x \in R \,|\, v(x) = (m,n) \in \mathbf{Z}^2,\ m \geq 1\}.$$

Let

$$f = \sum_{n\geq 0} ba^{-n}X^n, \quad g = a - X.$$

Then $fg = ab$ and so $c(fg) = (ab)$ but $c(g) = R$ and

$$c(f) = (b, ba^{-1}, ba^{-2}, \ldots) = \mathfrak{n}.$$

Note that in this case $c(f)c(g) \neq c(fg)$ but $c(f)^2c(g) = c(f)c(fg) = \mathfrak{n}^2$. Note also that while the ideal $c(g)$ is finitely generated, the ideal $c(f)$ is not.

These two examples show that the question posed by Epstein and Shapiro in Section 4 of [ES] has a negative answer *for the value of k stated there*. Furthermore, it hints at the fact that the statement of the Dedekind–Mertens lemma might fail not only because the ideal $c(g)$ is not finitely generated, but also because the ideal $c(f)$ is not finitely generated. In the next section, we will give some positive results concerning this question.

3. Main results. In this section, we state the main positive results that hopefully make the problem of Epstein–Shapiro clearer. We include only the statements, not the proofs.

The first statement is a mild generalization of Epstein–Shapiro to the case of non-noetherian rings of coefficients.

Theorem 3.1. *Let R be any ring and let $f, g \in R[\![X]\!]$, $g \neq 0$. Assume that the ideals $c(f)$ and $c(g)$ are locally finitely generated and let $k = \max_{\mathfrak{m}} \mu(c(g)R_{\mathfrak{m}})$ be the minimal local number of generators of $c(g)$. Assume $k < \infty$. Then*

$$c(f)^k c(g) = c(f)^{k-1}c(fg).$$

This theorem explains the failure of the Dedekind–Mertens lemma in Examples 2.4 and 2.5: it is due to the fact that the corresponding ideals $c(f)$ are not finitely generated. However, note that in both these examples the equality $c(f)^k c(g) = c(f)^{k-1}c(fg)$ still holds for $k = 2$ (rather than for $k = 1$, the number of local generators of $c(g)$ in these examples). We will now explain this phenomenon and show that in the case when $c(f)$ is not assumed to be finitely generated, we still have the following following weaker result.

THEOREM 3.2. *Let R be any ring and let $f, g \in R[\![X]\!]$, $g \neq 0$. Assume that the ideal $c(g)$ is finitely generated ($c(f)$ is allowed not to be finitely generated). Write $g = \sum_{i=0}^{\infty} b_i X^i$ and take k to be the number of $i \geq 0$ such that b_i does not lie in the ideal $(b_0, \ldots, b_{i-1})$ (for $i = 0$, this condition means that $b_0 \neq 0$). Then*

$$c(f)^k c(g) = c(f)^{k-1} c(fg).$$

Note that in Examples 2.4 and 2.5 we have $k = 2$, which explains the equalities $c(f)^2 c(g) = c(f)c(fg)$. This result is similar to a result proven by R. Gilmer, A. Grams, and T. Parker in [GGP], Theorem 3.6. In their result, g is assumed to be a polynomial and k is taken to be a number of nonzero monomials in g, so in this sense Theorem 3.2 is stronger than the result of Gilmer–Grams–Parker. It should be noted, however, that Gilmer, Grams, and Parker state their result also for power series in an arbitrary (possibly even infinite) number of variables (for details, see [GGP]).

We have already seen that the question of Epstein–Shapiro has a negative answer for the stated value of k. However, the following modified question is still valid.

QUESTION 3.3. *Let R be a ring and let $f, g \in R[\![X]\!]$. Assume that the ideal $c(g)$ is locally finitely generated and further assume that there is a common bound on the number of local generators. Does there exist an integer $k \geq 1$ such that $c(f)^k c(g) = c(f)^{k-1} c(fg)$?*

By Theorem 3.2, we know that the answer to this question is positive if R is local. We suspect that the answer is negative in general. However, in order to construct a counterexample, we would need to find a ring R and power series $f, g \in R[\![X]\!]$ such that

(i) The ideal $c(f)$ is not finitely generated (and not even locally finitely generated for infinitely many maximal ideals $\mathfrak{m}$). In particular, infinitely many localizations $R_{\mathfrak{m}}$ are non-noetherian.

(ii) The ideal $c(g)$ is locally finitely generated and there is a common bound on the number of such generators.

(iii) The ideal $c(g)$ is not finitely generated. Furthermore, if we write $g = \sum_{i=0}^{\infty} b_i X^i$, the number of proper *jumps* in the sequence

$$0 \subseteq (b_0) \subseteq (b_0, b_1) \subseteq (b_0, b_1, b_2) \subseteq \ldots \tag{1}$$

is locally arbitrarily large, i.e., for any $N \geq 0$ there is a maximal ideal $\mathfrak{m}$ of R such that in the sequence (1) localized in $\mathfrak{m}$ the number of proper inclusions is at least N.

Acknowledgments. The author gratefully acknowledges the support of the National Science Centre (NCN) under grant no. DEC-2012/07/E/ST1/00185.

References

[CVV] A. Corso, W. V. Vasconcelos, R. Villarreal, *Generic Gaussian ideals*, J. Pure Appl. Algebra 125 (1998), 117–127.

[D] R. Dedekind, *Über einen arithmetischen Satz von Gauss*, Gesammelte Werke XXII, Vol. 2, Mitt. Deutsch. Math. Ges. Prague (1892), 1–11.

[ES] N. Epstein, J. Shapiro, *A Dedekind–Mertens theorem for power series rings*, Proc. Amer. Math. Soc. 144 (2016), 917–924.

[F] D. E. Fields, *Zero divisors and nilpotent elements in power series rings*, Proc. Amer. Math. Soc. 27 (1971), 427–433.

[GGP] R. Gilmer, A. Grams, T. Parker, *Zero divisors in power series rings*, J. Reine Angew. Math. 278/279 (1975), 145–164.

[HH] W. Heinzer, C. Huneke, *The Dedekind–Mertens lemma and the contents of polynomials*, Proc. Amer. Math. Soc. 126 (1998), 1305–1309.

[K] L. Kronecker, *Zur Theorie der Formen höherer Stufen*, Monatsber. Akad. Wiss. Berlin (1883), 957–980.

[M] F. Mertens, *Über einen algebraischen Satz*, Sitzungsber. Akad. Wiss. Wien (2a) 101 (1892), 1560–1566.

[R] D. E. Rush, *Content algebras*, Canad. Math. Bull. 21 (1978), 329–334.