PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 5, May 1998, Pages 1305–1309
S 0002-9939(98)04165-3

THE DEDEKIND-MERTENS LEMMA AND THE CONTENTS OF POLYNOMIALS

WILLIAM HEINZER AND CRAIG HUNEKE

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. We prove a sharpening of the Dedekind-Mertens Lemma relating the contents of two polynomials to the content of their product. We show that for a polynomial g the integer $1+\deg(g)$ in the Dedekind-Mertens Lemma may be replaced by the number of local generators of the content of g. We also raise a question concerning the converse.

1. INTRODUCTION

Let R be a commutative ring and let t be an indeterminate over R. The *content* $c(f)$ of a polynomial $f \in R[t]$ is the ideal of R generated by the coefficients of f. The *Dedekind-Mertens Lemma* states that if $f = a_0 + a_1t + \cdots + a_mt^m$ and $g = b_0 + b_1t + \cdots + b_nt^n$ are polynomials in $R[t]$, then

$$c(f)^n c(f)c(g) = c(f)^n c(fg). \tag{1.1}$$

Since $c(f)c(g) \supseteq c(fg)$, the right hand side of (1.1) is always included in the left hand side. For a given polynomial $g \in R[t]$, it is natural to ask about a sharper form of Dedekind-Mertens in the sense of the following definition.

Definition 1.2. The *Dedekind-Mertens number* $\mu(g)$ of a polynomial $g \in R[t]$ is the smallest positive integer k such that

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

for every polynomial $f \in R[t]$.

Observe that the Dedekind-Mertens number of a polynomial $g(t)$ very much depends upon the coefficient ring R. It is not invariant under base change; indeed we know little of the behavior of this number even under faithfully flat extension. The Dedekind-Mertens Lemma says that $\mu(g) \leq \deg(g)+1$, the maximal number of coefficients of g. It is shown in [CVV, Theorem 2.1] that if f and g are polynomials with indeterminate coefficients over a field, then $\mu(g) = \deg(g) + 1$. But for many polynomials g, the Dedekind-Mertens number $\mu(g)$ is smaller than $\deg(g) + 1$. For example, polynomials g having Dedekind-Mertens number $\mu(g) = 1$ are precisely the *Gaussian polynomials*, i.e., the polynomials g such that $c(f)c(g) = c(fg)$ for every $f \in R[t]$. An interesting conjecture of Tsang-Glaz-Vasconcelos [GV] states

Received by the editors July 9, 1996 and, in revised form, October 23, 1996.
1991 *Mathematics Subject Classification.* Primary 13A15, 13B25, 13G05, 13H10.
Key words and phrases. Dedekind-Mertens Lemma, content of a polynomial.
The second author was partially supported by the NSF.

that a nonzero Gaussian polynomial over an integral domain has an invertible content ideal. Glaz and Vasconcelos establish the truth of this conjecture over all normal Noetherian integral domains in [GV], and it is shown to be true over all Noetherian domains in [HH].

In this paper we discuss a question which at the same time generalizes the classical Dedekind-Mertens Lemma[1] and the result concerning Gaussian polynomials described in the paragraph above. Our motivating question is:

Question 1.3. Let $(R, \mathbf{m})$ be an excellent local domain, and let $g \in R[t]$. Is $\mu(g) = \mu(c(g))$?

Here, $\mu(I)$ denotes the minimal number of generators of an ideal I. This question extends both of the theorems discussed above. We think of (1.3) as two separate questions: namely we divide the equality into two inequalities in opposite directions.

First consider the inequality $\mu(g) \leq \mu(c(g))$. In general $\mu(c(g)) \leq \deg(g) + 1$, so this inequality is a generalization of the classical lemma of Dedekind and Mertens.[2] The inequality $\mu(g) \leq \mu(c(g))$ should have nothing to do with the assumptions on the ring in (1.3): this inequality should be universal, and the veracity of this inequality is the main theorem of this paper, Theorem 2.1 below.

The other inequality, $\mu(c(g)) \leq \mu(g)$, is considerably less clear. The case in which $\mu(g) = 1$ would say that $\mu(c(g)) = 1$, i.e. it would say that Gaussian polynomials have locally principal content ideals. This is the content of the theorems in [GV] and [HH] cited above, since over an integral domain a finitely generated ideal is invertible iff it is locally principal (and nonzero). This inequality needs some condition on the ring. The ring should be local, since the definition of $\mu(g)$ localizes, while the number of generators of ideals may change greatly under localization. Moreover, the question has a negative answer in general over zero-dimensional rings. For example, if the maximal ideal $\mathbf{m}$ of R is not principal and $\mathbf{m}^2 = (0)$, then it is easily seen that there exist polynomials $g \in R[t]$ such that $\mu(g) < \mu(c(g))$, i.e., a generalization of (1.3) to this setting is false. Evidence is scanty for this direction. However, the case where f and g are both generic polynomials over a field is proved in [CVV, Theorem 2.1].

---

[1]The history of the Dedekind-Mertens Lemma is interesting. In [Ed, page 2], Edwards states that the theorem which Dedekind proved (see [De]) said that if f and g are polynomials whose coefficients are algebraic numbers such that the coefficients of fg are algebraic integers, then the product of any coefficient of f with an arbitrary coefficient of g is also an algebraic integer. In modern language this is just saying that the ideal $c(f)c(g)$ is integral over the ideal $c(fg)$, a theorem which is considerably weaker than what is now known as the Dedekind-Mertens Lemma. Apparently the fact that there exists an N such that $c(f)^N c(f)c(g) = c(f)^N c(fg)$ was known to Mertens, Kronecker [Kro], and perhaps Hurwitz [Hu]. Mertens' proof in 1892 shows that in characteristic 0, the number N can be chosen approximately equal to $\deg(g)^2$. However, the precise value of $N = \deg(g)$ was given by Dedekind in his 1892 paper [De, page 10]. Prüfer reproved this theorem with $N = \deg(g)$ [Pr, page 24] in 1932. The earliest reference we have found with the name 'Dedekind-Mertens Lemma' is in Krull [Kru, page 128]. It is interesting that the theorem Krull states as the Dekekind-Mertens Lemma has the value N equal to the sum of the degrees of f and g. In an article in 1959 [N] Northcott says he has not been able to find a reference for the Dedekind-Mertens Lemma and gives a proof he attributes to Emil Artin. Arnold and Gilmer [AG] give a proof and generalization whose idea we use in this paper.

[2]Gilmer, Grams and Parker [GGP, Theorems 3.6, 3.7] and Anderson and Kang [AK] prove and generalize that if g has $k+1$ nonzero terms, then $c(f)^k c(f)c(g) = c(f)^k c(fg)$ holds for all polynomials $f \in R[t]$; i.e., in our terminology, the Dedekind-Mertens number of g is bounded above by the number of nonzero coefficients of g. Theorem 2.1 below sharpens this by replacing the number of nonzero coefficients by the number of local generators.

All rings we consider are assumed to be commutative with identity and our notation is as in [M].

2. An upper bound on the Dedekind-Mertens number

The following is the main result of this paper.

Theorem 2.1. *Let R be a commutative ring, let $g \in R[t]$ be a polynomial, and let $c(g)$ denote the content ideal of g. If for each maximal ideal $\mathbf{m}$ of R, $c(g)R_{\mathbf{m}}$ is generated in $R_{\mathbf{m}}$ by k elements, then the Dedekind-Mertens number $\mu(g) \leq k$.*

Proof. Since $c(f)^n c(f)c(g) = c(f)^n c(fg)$ holds in R if and only if $c(f)^n c(f)c(g)R_{\mathbf{m}} = c(f)^n c(fg)R_{\mathbf{m}}$ for each maximal ideal $\mathbf{m}$ of R, the Dedekind-Mertens number $\mu(g)$ is the maximum of the Dedekind-Mertens numbers of the image of g in $R_{\mathbf{m}}[t]$ as $\mathbf{m}$ varies over the maximal ideals of R. Thus we may assume that the ring R is local (but not necessarily Noetherian), and it suffices to prove the following:

Lemma 2.2. *Let $(R, \mathbf{m})$ be a local ring and let $g \in R[t]$ be a polynomial. If the content ideal $c(g)$ of g is minimally generated by k elements, then the Dedekind-Mertens number $\mu(g) \leq k$, i.e., for every polynomial $f \in R[t]$ we have*

$$c(f)^{k-1}c(f)c(g) \subseteq c(f)^{k-1}c(fg). \tag{2.3}$$

We prove (2.2) by induction on k, the case $k = 1$ follows by factoring out the principal content of g and using the lemma of Gauss that says that a polynomial with unit content is Gaussian.

The following lemma implies we may assume that every nonzero coefficient of g is a minimal generator of $c(g)$.

Lemma 2.4. *Let $(R, \mathbf{m})$ be a local ring and let $g \in R[t]$ be a polynomial. Suppose $b \in R$ is such that $b \in \mathbf{m}c(g)$. Let i be a nonnegative integer and set $h = g + bt^i$. Let $\mathbf{a}$ be a finitely generated ideal of R and $f \in R[t]$ a polynomial. If $\mathbf{a}c(f)c(h) = \mathbf{a}c(fh)$, then also $\mathbf{a}c(f)c(g) = \mathbf{a}c(fg)$. Therefore g and h have the same Dedekind-Mertens number, i.e., $\mu(g) = \mu(h)$. More generally, if g^* and h^* are polynomials in $R[t]$ and if $c(g^* - h^*) \subseteq \mathbf{m}c(g^*)$, then $\mu(g^*) = \mu(h^*)$.*

Proof of (2.4). It is clear that $\mathbf{a}c(f)c(g) \supseteq \mathbf{a}c(fg)$. For the reverse inclusion, since $b \in \mathbf{m}c(g)$ and $h = g + bt^i$, we have $c(g) = c(h)$ by Nakayama's Lemma. Thus

$$\begin{aligned}\mathbf{a}c(f)c(g) = \mathbf{a}c(f)c(h) = \mathbf{a}c(fh) = \mathbf{a}c(f(g + bt^i)) &\subseteq \mathbf{a}(c(fg) + bc(f)) \\ &\subseteq \mathbf{a}c(fg) + \mathbf{ma}c(f)c(g).\end{aligned}$$

Nakayama's Lemma [M, page 8] implies $\mathbf{a}c(f)c(g) = \mathbf{a}c(fg)$. Letting $\mathbf{a} = c(f)^k$, we see that $\mu(g) \leq \mu(h)$. Since $g = h + (-b)t^i$, we also have $\mu(h) \leq \mu(g)$. If $c(g^* - h^*) \subseteq \mathbf{m}c(g^*)$, then h^* is obtained from g^* by a finite sequence of operations $h_j = g_j + b_j t^{i_j}$, where $b_j \in \mathbf{m}c(g_j) = \mathbf{m}c(g^*)$. Therefore $\mu(g^*) = \mu(h^*)$. □

Proof of (2.2). Assume that $c(g)$ is minimally generated by $k \geq 2$ elements and that for every polynomial $h \in R[t]$ minimally generated by less than k elements, we have for every polynomial $f \in R[t]$ that

$$c(f)^{k-2}c(f)c(h) \subseteq c(f)^{k-2}c(fh).$$

Our inductive step employs a technique used in [AG]. Let $g = b_m t^m + \cdots + b_1 t + b_0$. By (2.4), we may assume that b_m is a minimal generator of $c(g)$. Write $g = b_m h(t) + g_1(t)$, where $c(h) = R$ and $c(g_1)$ is generated by less than k elements. Also

write $f(t) = a_n t^n + f_1(t)$, where $\deg(f_1) < \deg(f) = n$. By induction on $\deg(f)$, we may assume $c(f_1)^k c(g) = c(f_1)^{k-1} c(f_1 g)$.

Claim 2.5. $c(fg_1) \subseteq c(fg) + b_m c(f_1)$.

Proof. We have

$$c(fg_1) = c(f(g - b_m h)) \subseteq c(fg) + c(b_m fh) = c(fg) + b_m c(fh) = c(fg) + b_m c(f)$$
$$= c(fg) + b_m c(a_n t^n + f_1(t)) \subseteq c(fg) + a_n b_m R + b_m c(f_1) = c(fg) + b_m c(f_1),$$

the last equality on the first line since $c(h) = R$ and the last equality on the second line since $a_n b_m \in c(fg)$. □

Claim 2.6. $c(f_1 g) \subseteq c(fg) + a_n c(g_1)$.

Proof. We have

$$c(f_1 g) = c((f - a_n t^n)g) \subseteq c(fg) + a_n c(t^n g) \subseteq c(fg) + a_n c(g)$$
$$\subseteq c(fg) + a_n c(b_m h(t) + g_1(t)) \subseteq c(fg) + a_n b_m R + a_n c(g_1) = c(fg) + a_n c(g_1),$$

the last equality since $a_n b_m \in c(fg)$. □

We now establish (2.3). It suffices to show each term in $c(f)^{k-1} c(f) c(g) = c(f)^k c(g)$ of the form $\theta = a_0^{v_0} \cdots a_n^{v_n} b_j$, where $\sum v_i = k$, is in $c(f)^{k-1} c(fg)$. Since $g = b_m h(t) + g_1(t)$, we can write $b_j = b_m e_j + b_{1j}$, where e_j is the coefficient of t^j in $h(t)$ and b_{1j} is the coefficient of t^j in $g_1(t)$.

Consider the following cases:

(2.7). Suppose $v_n \neq 0$ and $j = m$. Then $\theta = a_0^{v_0} \cdots a_n^{v_n - 1} a_n b_m \in c(f)^{k-1} c(fg)$.

(2.8). Suppose $v_n \neq 0$ and $j < m$. Then

$$\theta = a_0^{v_0} \cdots a_n^{v_n} b_j = a_0^{v_0} \cdots a_n^{v_n} (b_m e_j + b_{1j}) = a_0^{v_0} \cdots a_n^{v_n - 1} a_n b_m e_j$$
$$+ a_0^{v_0} \cdots a_n^{v_n - 1} a_n b_{1j} \in c(f)^{k-1} c(fg) + c(f)^{k-1} a_n c(g_1).$$

(2.9). Suppose $v_n = 0$. Then $\theta \in c(f_1)^k c(g) = c(f_1)^{k-1} c(f_1 g)$ by induction on the degree of f.

Combining these three cases, we have

$$c(f)^k c(g) \subseteq c(f)^{k-1} c(fg) + c(f)^{k-1} a_n c(g_1) + c(f_1)^{k-1} c(f_1 g)$$
$$\subseteq c(f)^{k-1} c(fg) + c(f)^{k-1} a_n c(g_1) + c(f_1)^{k-1} (c(fg) + a_n c(g_1)) \quad \text{(by (2.6))}$$
$$\subseteq c(f)^{k-1} c(fg) + c(f)^{k-1} a_n c(g_1) \qquad (\text{since } c(f_1) \subseteq c(f))$$

Since $c(g_1)$ is generated by less than k elements, we have $c(f)^{k-1} c(g_1) = c(f)^{k-2} c(fg_1)$ by induction on k. Therefore

$$c(f)^k c(g) \subseteq c(f)^{k-1} c(fg) + a_n c(f)^{k-2} c(fg_1)$$
$$\subseteq c(f)^{k-1} c(fg) + a_n c(f)^{k-2} (c(fg) + b_m c(f_1)) \qquad \text{(by (2.5))}$$
$$\subseteq c(f)^{k-1} c(fg).$$

This completes the proof of Theorem 2.1 □

Added in Proof

Concerning Question 1.3, in a joint paper with Alberto Corso entitled "A generalized Dedekind-Mertens Lemma and its converse" to appear in Trans. Amer. Math. Soc., we have shown (1.3) has an affirmative answer under suitable dimensionality restrictions, and that it is not true in general.

References

[AG] J. Arnold and R. Gilmer, *On the contents of polynomials*, Proc. Amer. Math. Soc. **24** (1970), 556–562. MR **40:**5581

[AK] D. D. Anderson and B. G. Kang, *Content formulas for polynomials and power series and complete integral closure*, J. Algebra **181** (1996), 82–94. MR **97c:**13014

[CVV] A. Corso, W. Vasconcelos and R. Villarreal, *Generic Gaussian ideals*, J. Pure Appl. Algebra (to appear).

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

[Ed] H. Edwards, *Divisor Theory*, Birkhäuser, Boston, 1990. MR **93h:**11115

[GGP] R. Gilmer, A. Grams, and T. Parker, *Zero divisors in power series rings*, Jour. reine angew. Math. **278/79** (1975), 145–164. MR **52:**8117

[GV] S. Glaz and W. Vasconcelos, *The content of Gaussian polynomials*, J. Algebra (to appear).

[HH] W. Heinzer and C. Huneke, *Gaussian polynomials and content ideals*, Proc. Amer. Math. Soc. **125** (1997), 739–745. MR **97e:**13015

[Hu] A. Hurwitz, *Ueber einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen*, Nachr. kön Ges. Wiss. Göttingen (1895), 230–240.

[Kro] L. Kronecker, *Zur Theorie der Formen höherer Stufen*, Monatsber Akad. Wiss. Berlin (1883), 957–960.

[Kru] W. Krull, *Idealtheorie, Zweite, ergänzte Auflage*, Springer-Verlag, Berlin, 1968. MR **37:**5197

[M] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986. MR **88h:**13001

[Mer] F. Mertens, *Über einen algebraischen Satz*, S.-B. Akad. Wiss. Wien (2a) **101** (1892), 1560–1566.

[N] D.G. Northcott, *A generalization of a theorem on the content of polynomials*, Proc. Cambridge Philos. Soc. **55** (1959), 282–288. MR **22:**1600

[Pr] H. Prüfer, *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, J. Reine Angew. Math. **168** (1932), 1–36.

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907-1395
E-mail address: heinzer@math.purdue.edu

E-mail address: huneke@math.purdue.edu