

TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SER. A

I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA

183

**SOME FORMULAE FOR MULTIPLYING
AND INVERTING IDEALS**

BY

J. PAHIKKALA

Turku 1982
TURUN YLIOPISTO

SOME FORMULAE FOR MULTIPLYING AND INVERTING IDEALS

Introduction

1. Let R be a subring of a commutative ring T . Denote by M_p the R -submodule of T generated by the coefficients of a polynomial p in $T[x]$. Arnold and Gilmer [1] have shown that if f and g are two polynomials in $T[x]$, then there is a non-negative integer k satisfying the condition

$$(1) \quad M_f^{k+1} M_g = M_f^k M_{fg}.$$

Supposing that the ring R contains a regular element and that T is the total quotient ring of R , the modules M_p are finitely generated fractional ideals of R . If in this case the factor M_f^k occurring on the both sides of (1) can be cancelled, then the equation (1) yields the multiplication formula

$$(2) \quad M_f M_g = M_{fg}$$

or

$$(2)' \quad (a_1, \dots, a_m)(b_1, \dots, b_n) = (a_1 b_1, a_1 b_2 + a_2 b_1, \dots, a_m b_n).$$

The cancellation is possible always when R is a Prüfer ring (see e.g. [9], p. 237) and the fractional ideal M_f regular. The rule (2) is well known for algebraic number fields (cp. e.g. [7], p. 105).

Conversely, it follows from the rule (2), even in a weakened form, that the ring under consideration is a Prüfer ring. This is proved in the present paper.

We also give a simplified proof of the above result of Arnold and Gilmer.

Moreover, we show the usefulness of the elementary division formula

$$\left[A: \sum_i A_i \right] = \bigcap_i [A: A_i]$$

for R -modules in deriving certain results for invertible fractional ideals. Especially, by using this formula we find a good bound for the number of generators of the intersection $A \cap B$ and by using also (2) a similar bound for the quotient $A:B$ whenever A and B are finitely generated regular fractional ideals of a Prüfer ring.

I wish to thank my venerable teacher Professor K. INKERI for the revision of this work and for his valuable advice.

2. Recall the definition of the invertible fractional ideal. If R is a commutative ring containing a regular element and if T is the total quotient ring of R , then we denote by R' the subring of T generated by R and the unity e of T . The ring $R' = R + \mathbf{Z}e$ is a principal fractional ideal of R , and even the identity in the multiplicative semigroup of the fractional ideals.

A fractional ideal A of the ring R is said to be *invertible* if there exists a fractional ideal B of the same ring such that the equation $AB = R'$ is valid (see [3], § 6). We shall make use of the facts about invertibility given in

Lemma 1. Let R be a commutative ring containing a regular element and let A be an invertible fractional ideal of R . Then the inverse of A , having the expression $[R':A]$,¹ is uniquely determined (and denoted by A^{-1}). Further, the fractional ideal A is finitely generated and regular. Furthermore, if A has a generating set of n elements, then the same is true for A^{-1} .

¹The *quotient* or *residual* $[B:C]$ of two R -submodules B and C of T is generally defined by

$$[B:C] = \{ t \in T: Ct \subseteq B \}$$

when R is a subring of a commutative ring T . The quotient is an R -submodule of T and, under the assumptions of paragraph 2, a fractional ideal of R in the case that B and C are such and C is regular (see [3], Theorem 6.1).

Proof. In [3] (Theorem 6.1) is found the proof of the first two assertions. Here we prove only the third assertion.

Thus we suppose the validity of the equations

$$AB = R', \quad A = (a_1, \dots, a_n).$$

The former equation implies the existence of the elements a'_i of A and b'_i of B ($i = 1, \dots, m$) such that $a'_1 b'_1 + \dots + a'_m b'_m = e$. But because

$$a'_i \in (a_1, \dots, a_n) = R'a_1 + \dots + R'a_n, \quad ,$$

so we have the expressions

$$a'_i = \sum_{j=1}^n r'_{ij} a_j,$$

where r'_{i1}, \dots, r'_{in} are elements of R' ($i = 1, \dots, m$). Now the unity of T acquires the form

$$e = \sum_{i=1}^m a'_i b'_i = \sum_{i=1}^m \sum_{j=1}^n r'_{ij} a_j b'_i = \sum_{j=1}^n a_j \sum_{i=1}^m r'_{ij} b'_i = \sum_{j=1}^n a_j b_j,$$

in which

$$b_j = \sum_{i=1}^m r'_{ij} b'_i \in R'B = B \quad (j = 1, \dots, n).$$

If b is an arbitrary element of the inverse ideal B , then it satisfies the condition

$$b = \sum_{j=1}^n (a_j b) b_j \in R'b_1 + \dots + R'b_n = (b_1, \dots, b_n).$$

Consequently, $B \subseteq (b_1, \dots, b_n)$. Since the converse inclusion is apparent we have arrived at the wished goal

$$A^{-1} = (b_1, \dots, b_n).$$

We shall also utilize the following deeper result, proved by Griffin (see [6], Theorem 13 and its proof, or alternatively [9], Theorem 10.18 and its proof).

Lemma 2. Let R be a commutative ring with non-zero unity. Then R is a Prüfer ring if every (integral) ideal of R generated by two elements, of which at least one is regular, is invertible.

A theorem of Arnold and Gilmer and a characterization of Prüfer rings

3. Here we use the same notation of the coefficient modules M_p as in paragraph 1.

Theorem 1 (Arnold and Gilmer). Let R be a subring of a commutative ring T . If f and g are polynomials in $T[x]$, then there exists a non-negative integer n satisfying the condition

$$(3) \quad M_f^{n+1} M_g = M_f^n M_{fg}.$$

Proof. We may presume that neither f nor g is the zero polynomial, since otherwise all values of n would satisfy (3). Now let n be the degree of g . Because the relation $M_{fg} \subseteq M_f M_g$ is trivially true we obtain the inclusion

$$M_f^n M_{fg} \subseteq M_f^{n+1} M_g.$$

We will prove the reverse inclusion

$$(4) \quad M_f^{n+1} M_g \subseteq M_f^n M_{fg}$$

by induction on the degree m of f and the degree n of g .

When m or n equals zero, then the corresponding polynomial is constant, and (3) is immediately established.

For the induction proof we assume the existence of the positive integers r and s such that (4) holds in the cases

$$m = r, \quad n < s$$

and

$$m < r, \quad n = s.$$

Now let the polynomials f and g be of the form

$$f = a_0 + a_1x + \dots + a_r x^r, \quad g = b_0 + b_1x + \dots + b_s x^s,$$

where a_r and b_s are distinct from zero. In order to prove the validity of the inclusion

$$(5) \quad M_f^{s+1} M_g \subseteq M_f^s M_{fg}$$

it suffices to show that the generators

$$c = a_0^{n_0} a_1^{n_1} \dots a_r^{n_r} b_j \quad (n_0 + n_1 + \dots + n_r = s + 1, \quad 0 \leq j \leq s)$$

of the left hand side of (5) belong to the right hand side.

In the case $n_r \geq 1, j = s$ we at once get the result

$$c = a_0^{n_0} a_1^{n_1} \dots a_r^{n_r-1} (a_r b_s) \in M_f^s M_{fg}.$$

We introduce the notations

$$f - a_r x^r = f_1, \quad g - b_s x^s = g_1.$$

Then the identity $f g_1 = f g - b_s f x^s$ implies the containment

$$(6) \quad M_{fg_1} \subseteq M_{fg} + b_s M_f$$

and the identity $f_1 g = (f g - a_r b_s x^{r+s}) - a_r g_1 x^r$ the containment

$$(6)' \quad M_{f_1 g} \subseteq M_{fg} + a_r M_{g_1}.$$

In the case $n_r \geq 1, j < s$ the element c belongs to the module $a_r M_f^s M_{g_1}$. If the polynomial g_1 does not vanish, then its degree t is at most equal to $s-1$, and therefore the induction hypothesis guarantees us the inclusion

$$(7) \quad M_f^{t+1} M_{g_1} \subseteq M_f^t M_{fg_1}.$$

Multiplying both sides of (7) by the expression $a_r M_f^{s-1-t}$ and applying (6) yields us

$$a_r M_f^s M_{g_1} \subseteq a_r M_f^{s-1} M_{fg} + M_f^s (a_r b_s)$$

and thus evidently

$$(8) \quad a_r M_f^s M_{g_1} \subseteq M_f^s M_{fg},$$

which holds also when g_1 is the zero polynomial. So c is in $M_f^s M_{fg}$.

We still have to treat the case $n_r = 0$. Now the element c is in the module $M_{f_1}^{s+1} M_g$, which, by the induction hypothesis, is contained in the module $M_{f_1}^s M_{f_1 g}$. Making use of the inclusion $M_{f_1} \subseteq M_f$ and of (6)' gives us the relation

$$c \in M_f^s M_{f_1 g} \subseteq M_f^s M_{fg} + a_r M_f^s M_{g_1}.$$

Here the condition (8) again shows that also this time the generator c must lie in the module $M_f^s M_{fg}$.

4. From the definition of the Prüfer ring and from the preceding theorem follows the “only if”-part of

Theorem 2. Let R be a commutative ring with non-zero unity and T be the total quotient ring of R . Then R is a Prüfer ring if and only if the equation

$$(9) \quad M_f M_g = M_{fg}$$

holds whenever f and g belong to the polynomial ring $T[x]$ and at least one of the fractional ideals M_f and M_g is regular.

Gilmer (see [2], pp. 240–241, and [3], p. 335) has established this characterization theorem for Prüfer rings in the case that the ring R is an integral domain. We next state the “if”-part of theorem 2 in a stronger two-generator form. The proof remains simple, except that it requires the use of lemma 2. Especially need the integral closedness of the ring R not be shown (cp. [2] and [3]).

Theorem 3. The commutative ring R with non-zero unity is a Prüfer ring if the multiplication rule

$$(9)' \quad (a, b)(c, d) = (ac, ad+bc, bd)$$

for the integral ideals of R holds whenever at least one of the generators a, b, c and d is regular.

Proof. Consider two arbitrary elements a and b of the ring R such that at least one of them, e.g. the element a , is regular. By the lemma 2, it is sufficient to show that the integral ideal (a, b) is invertible.

According to (9)', we first have

$$(a, b)^2 = (a, -b)(a, b) = (a^2, ab - ba, b^2) = (a^2, b^2).$$

Thus the product ab may be written in the form

$$ab = ua^2 + vb^2,$$

where u and v are elements of R . Again applying the rule (9)' gives

$$\begin{aligned} (a, b)(va, a-vb)(a^{-2}) &= (va^2, a^2 - vab + vab, ab - vb^2)(a^{-2}) = \\ &= (va^2, a^2, ua^2)(a^{-2}) = \\ &= (v, e, u) = \\ &= R. \end{aligned}$$

Consequently the ideal (a, b) has an inverse, which settles the proof.

Note. The rule (9)' in the theorem 3 can be replaced with the rule

$$(a, b)(c, d) = (ac, (a+b)(c+d), bd),$$

as is seen from the equation $(a+b)(c+d) - ac - bd = ad + bc$.

Applications of formula $[A: \sum_i A_i] = \bigcap_i [A: A_i]$

5. Suppose that R is a subring of a commutative ring T . If A_1, \dots, A_k and A are R -submodules of the ring T , then the division formula

$$(10) \quad [A: (A_1 + \dots + A_k)] = [A: A_1] \cap \dots \cap [A: A_k]$$

holds. The verification is straightforward (cp. e.g. [9], Proposition 2.3):

$$\begin{aligned} c \in [A: \sum_i A_i] &\Leftrightarrow \sum_i A_i c \subseteq A \\ &\Leftrightarrow A_i c \subseteq A \quad \forall i \\ &\Leftrightarrow c \in [A: A_i] \quad \forall i \\ &\Leftrightarrow c \in \bigcap_i [A: A_i]. \end{aligned}$$

Theorem 4. Let R be a commutative ring containing a regular element. If an invertible fractional ideal C of R is expressible as the sum of some invertible fractional ideals A_1, \dots, A_k , then the inverse of C necessarily has the expression

$$(11) \quad C^{-1} = A_1^{-1} \cap \dots \cap A_k^{-1}.$$

Proof. The fractional ideals A_i are R -submodules of the total quotient T of R . Therefore we can use the formula (10). Regarding also lemma 1 we obtain

$$C^{-1} = [R': C] = [R': (A_1 + \dots + A_k)] = [R': A_1] \cap \dots \cap [R': A_k] = A_1^{-1} \cap \dots \cap A_k^{-1}.$$

Gilmer and Heinzer ([5], p. 143) present formula (11) for the finitely generated non-zero fractional ideals of a Prüfer domain, as a consequence of Jensen's formula

$$(12) \quad (A + B)(A \cap B) = AB.$$

This formula characterizes the fractional ideals of the Prüfer domain (and Prüfer ring), but it requires a complicated derivation (see e.g. [8], p. 93).

Note. In the special case that the invertible fractional ideal C has a system of regular generators a_1, \dots, a_k , the equation (11) gives the result

$$(a_1, \dots, a_k)^{-1} = (a_1^{-1}) \cap \dots \cap (a_k^{-1}).$$

6. If R is as in theorem 4, and A and B are both regular fractional ideals of R , then one can without trouble ensure that the intersection $A \cap B$ is also regular. A Prüfer ring permits more:

Theorem 5. Assume that A and B are regular fractional ideals of a Prüfer ring R and have generating sets of m and n elements, respectively. Then the intersection $A \cap B$ and the quotient

$$A:B = \{ r \in R: Br \subseteq A \}$$

both have generating sets of $m+n$ elements.

Proof. Because A and B are finitely generated regular fractional ideals of a Prüfer ring, they are invertible. By lemma 1, the same is true for the sum $A^{-1} + B^{-1}$. Theorem 4 then gives the equation

$$(A^{-1} + B^{-1})^{-1} = A \cap B.$$

Furthermore, by the lemma 1, the sum $A^{-1} + B^{-1}$ and similarly also its inverse $A \cap B$ may be generated by $m+n$ elements.

It is not hard to show that the quotient $A:B$ has the presentation

$$(13) \quad A:B = AB^{-1} \cap R$$

(cp. e.g. [3], Proposition 21.4). The product AB^{-1} is obviously regular and, according to lemma 1 and theorem 2, it has a generating set of $m+n-1$ elements. Moreover, the ring R itself is regular and principal as an ideal. Hence we conclude that the intersection $AB^{-1} \cap R$ or the quotient $A:B$ has, by the first part of theorem 5, a generating set consisting of

$$(m+n-1)+1 = m+n$$

elements.

Gilmer and Heinzer give in [4] (p. 283) and [5] (p. 143) the bounds $m+n$ and $m(m+n)$ for the number of generators of $A \cap B$ and $A:B$, respectively. These concern the integral ideals of a Prüfer domain and are based on Jensen's formula (12). Also a better bound $mn+1$ for the number of generators of $A:B$, derivable from (13), is presented in the latter paper.

References

- [1] ARNOLD, J., and GILMER, R.: "On the contents of polynomials". – *Proc. Amer. Math. Soc.* 24 (1970), 556–562.
- [2] GILMER, R.: "Some applications of the *Hilfssatz von Dedekind–Mertens*". – *Math. Scand.* 20 (1967), 240–244.
- [3] GILMER, R.: "*Multiplicative ideal theory*". Queens University Press, Kingston, Ontario (1968).
- [4] GILMER, R., and HEINZER, W.: "Overrings of Prüfer domains II". – *J. Alg.* 7 (1967), 281–302.
- [5] GILMER, R., and HEINZER, W.: "On the number of generators of an invertible ideal". – *J. Alg.* 14 (1970), 139–151.
- [6] GRIFFIN, M.: "Prüfer rings with zero divisors". – *J. Reine Angew. Math.* 239/240 (1969), 55–67.
- [7] HECKE, E.: "*Vorlesungen über die Theorie der algebraischen Zahlen*". Chelsea Publishing Company, New York (1948).
- [8] JENSEN, C. U.: "On characterizations of Prüfer rings". – *Math. Scand.* 13 (1963), 90–98.

[9] LARSEN, M., and MCCARTHY, P.: “*Multiplicative theory of ideals*”. Academic Press, New York (1971).