# ON THE CONTENTS OF POLYNOMIALS

JIMMY T. ARNOLD AND ROBERT GILMER[1]

In [13, p. 24], Prüfer establishes the following result. (See also [2, Exercise 21, p. 97].)

*Let $J$ be an integral domain with identity having quotient field $K$ and let $f$, $g$, $h \in K[X]$ be such that $h=fg$. If $A$, $B$, and $C$ denote the fractional ideals of $J$ generated by the coefficients of $f$, $g$, and $h$, respectively, and if $n$ is the degree of the polynomial $g$, then $A^nC=A^{n+1}B$.*

This result is essentially what Krull in [7, p. 128] calls the *Hilfssatz von Dedekind-Mertens*, although the results which Dedekind in [4] and Mertens in [11] prove are not so general as Prüfer's theorem.

In this note, we generalize the theorem cited above, first to the case where $J$ is an arbitrary subring of the commutative ring $K$, and then to the case of polynomials in finitely many indeterminates. We conclude with some applications of the results obtained.

We use consistently the following notation in this paper. $R$ denotes a subring of a commutative ring $S$. If $f$ is a polynominal over $S$, $Y_f$ denotes the set of coefficients of $f$, and $A_f$ denotes the $R$-submodule of $S$ generated by $Y_f$; we call $A_f$ the *R-content of f*. The following result is straightforward, but we list it here for the sake of reference.

LEMMA 1. *If $f$ and $g$ are polynomials over $S$, and if $r \in R$, then*
(a) $A_{f+g} \subseteq A_f + A_g$,
(b) $A_{fg} \subseteq A_f A_g$, *and*
(c) $A_{rf} = rA_f$.

THEOREM 1. *Let $X$ be an indeterminate over $S$, and let $f$, $g \in S[X] - \{0\}$. If $m$ is the degree of $g$, then $A_f^{m+1}A_g = A_f^m A_{fg}$.*

PROOF. By Lemma 1 $A_{fg} \subseteq A_f A_g$; consequently, $A_f^m A_{fg} \subseteq A_f^{m+1} A_g$. We show that $A_f^{m+1}A_g \subseteq A_f^m A_{fg}$ by induction on $n$ and $m$, the degrees of $f$ and $g$, respectively.

Suppose that $f$ is a monomial; say $f=a_nX^n$, and let $g=b_0+b_1X+\cdots+b_mX^m$. Then

$$A_f^m A_{fg} = (a_n)^m(a_nb_0, \cdots, a_nb_m) = (a_n)^{m+1}(b_0, \cdots, b_m) = A_f^{m+1} A_g.$$

Similarly, if $g=b_mX^m$ and $f=a_0+a_1X+\cdots+a_nX^n$, we have

Received by the editors March 17, 1969.

[1] This research was done in 1966, while the second author was an Alfred P. Sloan Foundation Fellow.

$$\begin{aligned} A_f^m A_{fg} &= (a_0, \cdots, a_n)^m (a_0 b_m, \cdots, a_n b_m) \\ &= (a_0, \cdots, a_n)^{m+1} (b_m) = A_f^{m+1} A_g. \end{aligned}$$

Thus, if either $f$ or $g$ is a monomial, the theorem is true. In particular, if either $f$ or $g$ has degree zero the theorem holds.

If $h \in S[X]$, we denote by deg $h$ the degree of $h$. By induction we may now make the following assumptions.

(A) If deg $f = n < r$ and deg $g = m$, then $A_f^{m+1} A_g \subseteq A_f^m A_{fg}$.

(B) If deg $f = r$ and deg $g = m < s$, then $A_f^{m+1} A_g \subseteq A_f^m A_{fg}$.

Now let $f = a_0 + a_1 X + \cdots + a_r X^r$, $a_r \neq 0$, $g = b_0 + b_1 X + \cdots + b_s X^s$, $b_s \neq 0$, and suppose that neither $f$ nor $g$ is a monomial. Then we wish to show that $A_f^{s+1} A_g \subseteq A_f^s A_{fg}$.

Let $f_1 = f - a_r X^r$, $g_1 = g - b_s X^s$, $h = fg$, $h_1 = f_1 g$, and $h_2 = f g_1$. Then we have

$$h = \sum_{k=0}^{r+s} c_k X^k, \qquad c_k = \sum_{i+j=k} a_i b_j, \qquad 0 \leqq k \leqq r+s;$$

$$h_1 = \sum_{k=0}^{r+s-1} c_k^{(1)} X^k, \qquad c_k^{(1)} = c_k, \qquad 0 \leqq k \leqq r-1, \qquad \text{and}$$

$$c_k^{(1)} = c_k - b_{k-r} a_r, \qquad r \leqq k \leqq r+s-1;$$

$$h_2 = \sum_{k=0}^{r+s-1} c_k^{(2)} X^k, \qquad c_k^{(2)} = c_k, \qquad 0 \leqq k \leqq s-1, \qquad \text{and}$$

$$c_k^{(2)} = c_k - a_{k-s} g_s, \qquad s \leqq k \leqq r+s-1.$$

Then

$$\begin{aligned} A_{f_1 g} &= (c_0^{(1)}, \cdots, c_{r+s-1}^{(1)}) \\ &= (c_0, \cdots, c_{r-1}, c_r - b_0 a_r, \cdots, c_{r+s-1} - b_{s-1} a_r) \subseteq (c_0, \cdots, c_{r+s}) \\ &\quad + (a_r)(b_0, \cdots, b_{s-1}) = A_{fg} + a_r A_{g_1}, \end{aligned}$$

and

$$\begin{aligned} A_{fg_1} &= (c_0^{(2)}, \cdots, c_{r+s-1}^{(2)}) \\ &= (c_0, \cdots, c_{s-1}, c_s - a_0 b_s, \cdots, c_{r+s-1} - a_{r-1} b_s) \\ &\subseteq (c_0, \cdots, c_{r+s}) + (a_0, \cdots, a_{r-1})(b_s) \\ &= A_{fg} + b_s A_{f_1}. \end{aligned}$$

Since $A_f^{s+1} A_g$ is generated by elements of the form

$$\alpha = a_0^{n_0} a_1^{n_1} \cdots a_r^{n_r} b_i,$$

where $\sum_{j=0}^{r} n_j = s+1$ and $0 \leqq i \leqq s$, it suffices to show that each element of this form is contained in $A_f^s A_{fg}$. If $n_r \neq 0$ and $i=s$, then $\alpha = a_0^{n_0} a_1^{n_1} \cdots a_r^{n_r-1} c_{r+s}$, since $c_{r+s} = a_r b_s$. But $c_{r+s} \in A_{fg}$ so that $\alpha \in A_f^s A_{fg}$. If $n_r \neq 0$ and $i<s$, then $\alpha \in A_f^s(a_r) A_{g_1}$. Finally, in case $n_r = 0$ we have $\alpha \in A_{f_1}^{s+1} A_g$. Therefore,

$$A_f^{s+1} A_g \subseteq A_f^s A_{fg} + A_{f_1}^{s+1} A_g + A_f^s(a_r) A_{g_1}.$$

But by (A), $A_{f_1}^{s+1} A_g \subseteq A_{f_1}^s A_{f_1 g}$, and we have seen that $A_{f_1 g} \subseteq A_{fg} + a_r A_{g_1}$. Consequently, we have

$$A_{f_1}^{s+1} A_g \subseteq A_{f_1}^s A_{fg} + A_{f_1}^s (a_r) A_{g_1} \subseteq A_f^s A_{fg} + A_f^s (a_r) A_{g_1}.$$

Thus $A_f^{s+1} A_g \subseteq A_f^s A_{fg} + A_f^s(a_r) A_{g_1}$. By (B), if $\lambda = \deg g_1$, then $A_f^{\lambda+1} A_{g_1} \subseteq A_f^\lambda A_{fg_1}$. Since $\lambda \leqq s-1$, we have $A_f^s A_{g_1} \subseteq A_f^{s-1} A_{fg_1}$. But $A_{fg_1} \subseteq A_{fg} + b_s A_{f_1}$ so that

$$\begin{aligned} A_f^s(a_r) A_{g_1} &\subseteq A_f^{s-1}(a_r) A_{fg} + A_f^{s-1}(a_r)(b_s) A_{f_1} \subseteq A_f^s A_{fg} + c_{r+s} A_f^{s-1} A_{f_1} \\ &\subseteq A_f^s A_{fg}. \end{aligned}$$

Therefore, $A_f^{s+1} A_g \subseteq A_f^s A_{fg}$ as we wished to show.

It now follows by induction that if $\deg g = m$, then $A_f^{m+1} A_g \subseteq A_f^m A_{fg}$. Consequently, $A_f^{m+1} A_g = A_f^m A_{fg}$ and the proof is complete.

We now wish to extend the results of Theorem 1 to polynomial rings in finitely many indeterminates. We first prove a lemma.

Lemma 2. *Let $\{X_1, \cdots, X_n, X\}$ be a set of indeterminates over the ring $S$, and let $f, g \in S[X_1, \cdots, X_n, X] - \{0\}$. Then there exist $f^*$, $g^* \in S[X_1, \cdots, X_n] - \{0\}$ such that $Y_f = Y_{f^*}$, $Y_g = Y_{g^*}$, and $Y_{fg} = Y_{f^*g^*}$.*

Proof. Let $t(X_1, \cdots, X_n, X)$ be any element of $S[X_1, \cdots, X_n, X] - \{0\}$. We write $t$ as a polynomial in $X$ with coefficients in

$$S[X_1, \cdots, X_n]: \qquad t = \sum_{i=0}^{k} t_i X^i,$$

and we denote by $\partial_n t$ the degree of $t$ in $X_n$, which is equal to the maximum of the degrees of the $t_i$'s in $X_n$. We observe that if $m > \partial_n t$, then the coefficients of

$$t^* = t(X_1, \cdots, X_n, X_n^m) = \sum_{i=0}^{k} t_i X_n^{mi}$$

are the same as the coefficients of $t$. For if $0 \leqq i \leqq k$ and if $t_i \neq 0$, then $\partial_n t_i < m$ so that $mi \leqq \partial_n \xi < m(i+1)$ for any nonzero monomial $\xi$ of $t_i X_n^{mi}$. Therefore, the nonzero monomials appearing in $t_i X_n^{mi}$ are distinct from those appearing in $t_jX_n^{mj}$ for $i\neq j$. It follows that $t$ and $t^*$ have the same sets of coefficients.

We choose $m=\partial_n f+\partial_n g+1$. Then $m>\partial_n f$, $m>\partial_n g$, and $m>\partial_n fg$. The mapping $h(X_1, \cdots, X_n, X)\to h^*=h(X_1, \cdots, X_n, X_n^m)$ is a homomorphism of $S[X_1, \cdots, X_n, X]$ onto $S[X_1, \cdots, X_n]$. Therefore, $(fg)^*=f^*g^*$. And the results of the preceding paragraph show that $Y_f=Y_{f^*}$, $Y_g=Y_{g^*}$, and $Y_{fg}=Y_{f^*g^*}$.

THEOREM 2.[2] *If $f$, $g\in S[X_1, \cdots, X_n]-\{0\}$, then there exists a positive integer $k$ such that $A_f^{k+1}A_g=A_f^kA_{fg}$.*

PROOF. For $n=1$, the result follows from Theorem 1. If the result is true for $n=r$, and if $f$, $g\in S[X_1, \cdots, X_r, X_{r+1}]-\{0\}$, then Lemma 2 implies the existence of elements $f^*$, $g^*\in S[X_1, \cdots, X_r]$ such that $A_f=A_{f^*}$, $A_g=A_{g^*}$, and $A_{fg}=A_{f^*g^*}$. It then follows from the induction hypothesis that there is a positive integer $k$ such that $A_f^{k+1}A_g=A_f^kA_{fg}$.

We turn now to several applications of Theorem 2. In [10], McCoy has shown that if $f$ is a zero divisor in $S[X_1, \cdots, X_n]$, then there is a nonzero element $c$ of $S$ such that $cf=0$. This result is an easy consequence of Theorem 2,[3] for if $g$ is a nonzero element of $S[X_1, \cdots, X_n]$ such that $fg=0$, then by Theorem 2, there is a positive integer $k$ such that $A_f^{k+1}A_g=A_f^kA_{fg}=(0)$. We choose $t$ to be minimal positive such that $A_f^tA_g=(0)$. Then if $c$ is a nonzero element of $A_f^{t-1}A_g$ (if $t=1$, we set $A_f^{t-1}A_g=A_g$), we have $(0)=cA_f=A_{cf}$ so that $cf=0$.

An interesting case of Theorem 2 is that when $R$ is a commutative ring with identity and $S$ is the total quotient ring of $R$. In this case, $A_f$ is a fractional ideal of $R$. Thus if $A_f$ is invertible, then $A_fA_g=A_{fg}$ for any $g\in S[X_1, \cdots, X_n]$. In particular, if $R$ is a *Prüfer domain* (that is, an integral domain with identity over which each finitely generated fractional ideal is invertible) and if $S$ is the quotient field of $R$, then $A_fA_g=A_{fg}$ for any $f$, $g\in S[X_1, \cdots, X_n]$. It can be shown, in fact, that an integral domain $D$ with identity is a Prüfer domain if and only if $A_fA_g=A_{fg}$ for any $f$, $g\in D[X]$ (see [6, p. 241]).

If $R$ is a unique factorization domain (UFD) with quotient field $S$, then it is well known that each irreducible polynomial $f$ in $R[X_1, \cdots, X_n]$ is also irreducible in $S[X_1, \cdots, X_n]$. Our next result will show that any *Bezout domain*—that is, an integral domain with identity in which every finitely generated ideal is principal—

[2] The distinctive aspect of our Theorem 2 is in its method of proof; Northcott proves a more general result in [12].

[3] H. Tsang has made this same observation independently in her dissertation [14].

enjoys this same property. Since a Bezout domain is a UFD if and only if it is a principal ideal domain (PID), and since examples of Bezout domains which are not PID's are well known (for example, any valuation ring of rank greater than one, the ring of entire functions, or the ring of all algebraic integers), it will follow that the "invariance of irreducibility" condition mentioned above does not characterize UFD's among integral domains with identity. (A reasonable conjecture as to the class of integral domains with identity which are characterized by this invariance condition would be the domains over which every $v$-ideal of finite type is principal [**13**, p. 18], [**8**, p. 665], [**5**, §36], [**3**]. Such a domain satisfies the "invariance of irreducibility" condition, but the status of the converse is in doubt; in this connection, see the acknowledgment at the end of the paper.)

THEOREM 3. *Let $R$ be a Prüfer domain with quotient field $S$. If $R$ is a Bezout domain and if $n$ is a positive integer, then each element $f$ of $R[X_1, \cdots, X_n]$ irreducible in $R[X_1, \cdots, X_n]$ is also irreducible in $S[X_1, \cdots, X_n]$. Conversely, if for some positive integer $n$, each irreducible element of $R[X_1, \cdots, X_n]$ is irreducible in $S[X_1, \cdots, X_n]$, then $R$ is a Bezout domain.*

PROOF. If $R$ is Bezout and if $f$ factors as a product of two polynomials $g$, $h$ of positive degree in $S[X_1, \cdots, X_n]$, then $A_g = \xi R$ is a principal fractional ideal of $R$ and $A_f = A_g A_h = \xi A_h$. It follows that $f = \xi^{-1}g \cdot \xi h$ is a factorization, in $R[X_1, \cdots, X_n]$, of $f$ into a product of two polynomials of positive degree, for $A_{\xi^{-1}g} = \xi^{-1}A_g = R$ and $A_{\xi h} = \xi A_h = A_f$ so that $\xi^{-1}g$ and $\xi h$ are in $R[X_1, \cdots, X_n]$. This establishes the contrapositive of the first statement of Theorem 3.

We show, conversely, that if $R$ is a Prüfer domain which is not Bezout, then for any positive integer $n$, there is an element $f$ which is irreducible in $R[X_1, \cdots, X_n]$, but not irreducible in $S[X_1, \cdots, X_n]$. Hence, there are elements $a$, $b$ in $R$ such that $(a, b)$ is not principal. The fractional ideal $(a, b)^{-1}$ also has a basis $\{c, d\}$ of two elements, $(a, b)(c, d) = R$, and $(c, d)$ is not principal. The polynomial $f = (a + bX_1)(c + dX_1)$ is in $R[X_1, \cdots, X_n]$ since $A_f = (a, b)(c, d) = R$, $f$ obviously is not irreducible in $S[X_1, \cdots, X_n]$, but we show presently that $f$ is irreducible in $R[X_1, \cdots, X_n]$. Since $A_f = R$, $f$ has no nonunit factor of degree 0 in $R[X_1, \cdots, X_n]$. Further, since $S[X_1, \cdots, X_n]$ is a UFD and since $a + bX_1$ and $c + dX_1$ are irreducible in $S[X_1, \cdots, X_n]$, any factorization of $f$ into factors of positive degree in $R[X_1, \cdots, X_n]$ would necessarily be of the form $\xi(a + bX)$ $\cdot \xi^{-1}(c + dX)$ for some $\xi \in S - \{0\}$. Such a factorization over $R$, a Prüfer domain, would imply that $R = A_f = A_{\xi(a+bX)} A_{\xi^{-1}(c+dX)}$ so that

$R=A_{\xi(a+bX)}=\xi(a, b)$ and $(\xi)^{-1}=(a, b)$, a contradiction to the assumption that $(a, b)$ is not principal.

One final application of Theorem 2. In algebraic number theory, the ***norm of an ideal***, defined as follows [**9**, p. 68], is of basic importance. Let $K$ be a finite algebraic extension field of the rational field $Q$, let $Z^*$ be the ring of algebraic integers in $K$, and let $A^*$ be an ideal of $Z^*$. The ***norm of*** $A^*$, denoted by $N(A^*)$, is defined to be the ideal $\sigma_1(A^*)\sigma_2(A^*) \cdots \sigma_m(A^*)Z'$ of $Z'$, the ring of integers in $E$, a normal closure of $K/Q$ where $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$ is the Galois group of $E/Q$. It can be shown that $N(A^*)$ is principal and is generated by a rational integer. By using Theorem 2, we can generalize this result to any Prüfer domain as follows.

Let $D_0$ be a Prüfer domain with quotient field $K_0$, let $K_1$ be a finite algebraic extension field of $K_0$, and let $D_1$ be the integral closure of $D_0$ in $K_1$. If $E/K_0$ is a normal closure of $K_1/K_0$ with Galois group $\{\sigma_1=1, \cdots, \sigma_m\}$ and degree of inseparability $p^n$, where $p$ is the characteristic exponent of $K_0$, if $D$ is the integral closure of $D_0$ in $E$, and if $A=\{a_0, a_1, \cdots, a_v\}D_1$ is a finitely generated ideal of $D_1$, then we define the norm of $A$, $N(A)$, to be $[\sigma_1(A) \cdots \sigma_m(A)D]^{p^n}$. We prove

THEOREM 4. *$N(A)$ is the extension to $D$ of a finitely generated ideal of $D_0$; that is, $N(A)$ has a finite basis consisting of elements of $D_0$.*

PROOF. The domain $D$ is a Prüfer domain [**13**, p. 31]. We write $f_1=\sum_{j=0}^{v} a_jX^j$, and for $1\leqq i\leqq m$, $f_i=\sum_{j=0}^{v} \sigma_i(a_j)X^j$. For each $i$ we have $\sigma_i(A)D=A_{f_i}$ and $f_i=\sigma_i^*(f_1)$, where $\sigma_i^*$ is the automorphism on $D[X]$ which sends $X$ to $X$ and which restricts to $\sigma_i$ on $D$. Then by definition, $N(A)=[\sigma_1(A) \cdots \sigma_m(A)D]^{p^k}=[A_{f_1}A_{f_2} \cdots A_{f_m}]^{p^k}=A_f{}^{p^k}$ where $f=f_1f_2 \cdots f_m$. But it is apparent that $\sigma_i^*(f)=f$ for $1\leqq i\leqq m$ so that the coefficients of $f$ are in $D$ and are left fixed by each element of the Galois group of $E/K_0$. Consequently, $f^{p^k}\in D[X]\cap K_0[X]=(D\cap K_0)[X]=D_0[X]$. Therefore $N(A)=A_f{}^{p^k}$, has a finite basis consisting of elements of $D_0$.

ACKNOWLEDGMENT. We are grateful to the referee for pointing out to us that the conjecture concerning invariance of irreducibility, which was made in the paragraph preceding Theorem 3, is incorrect. To prove this, we recall some terminology from [**3**]. An element $c$ of an integral domain $D$ is said to be ***primal*** if $c\mid a_1a_2$ implies that $c=c_1c_2$, where $c_i\mid a_i$. A *Schreier ring* is an integrally closed domain in which each nonzero element is primal. If $R$ is a commutative ring with identity, and if $S$ is a commutative unitary overring of $R$, then $R$ is said to be ***inert*** in $S$ if for any nonzero element $c$ of $R$ and any factorization $c=ab$ of $c$ in $S$, there is a unit $u$ of $S$ such that $ua$ and

$u^{-1}b$ are in $R$. The referee has communicated to the authors a proof of the following result.

*Let $D$ be an integral domain with identity having quotient field $K$.*

(1) *If $D$ is a Schreier ring, then for any positive integer $n$, $D[X_1, \cdots, X_n]$ is inert in $K[X_1, \cdots, X_n]$.*

(2) *If $D[X_1, \cdots, X_n]$ is inert in $K[X_1, \cdots, X_n]$ for some $n \geqq 1$, then $D$ is a Schreier ring.*

If $R$ is inert in $S$, it is clear that each irreducible element of $R$ is also irreducible in $S$. Conversely, if each nonzero element of $R$ is a finite product of irreducible elements in $R$ (in the terminology of [3], this is the condition that $R$ be *atomic*), if irreducible elements of $R$ are irreducible in $S$, and if $S$ is a UFD, then $R$ is inert in $S$.

At any rate, a Schreier ring $D$ with quotient field $K$ is such that each irreducible element of $D[X_1, \cdots, X_n]$, for any $n$, is irreducible in $K[X_1, \cdots, X_n]$; the status of the converse is unclear, but Cohn in [3, p. 256] gives an example of a Schreier ring containing a $v$-ideal of finite type which is not principal.

## References

1. D. Boccioni, *Alcune osservazioni sugli anelli pseudo-bezoutiani e fattoriali*, Rend. Sem. Mat. Univ. Padova **37** (1967), 273–288. MR **36** #148.

2. N. Bourbaki, *Algebre commutative*. Chapitre 7, Hermann, Paris, 1965.

3. P. M. Cohn, *Bezout rings and their subrings*, Proc. Cambridge Philos. Soc. **64** (1968), 251–264. MR **36** #5117.

4. R. Dedekind, *Über einen arithmetischen Satz von Gauss*, Mitt. Deutsch. Math. Ges., Prague, 1892, pp. 1–11; *Gesammelte Werke* XXII. Vol. 2.

5. Robert Gilmer, *Multiplicative ideal theory*, Queen's Papers in Pure and Appl. Math., no. 12, Queen's University, Kingston, Ontario, 1968. MR **37** #5198.

6. ———, *Some applications of the Hilfssatz von Dedekind-Mertens*, Math. Scand. **20** (1967), 240–244.

7. W. Krull, *Idealtheorie*, Chelsea, New York, 1948.

8. ———, *Beiträge zur Arithmetik kommutativer Integritätsbereiche*. II, Math. Z. **41** (1936), 665–679.

9. H. B. Mann, *Introduction to algebraic number theory*, Ohio State Univ. Press, Columbus, Ohio, 1955. MR **17**, 240.

10. N. H. McCoy, *Remarks on divisors of zero*, Amer. Math. Monthly 49 (1942), 286–295. MR **3**, 262.

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

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

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

14. H. Tsang, *Gauss' lemma*, Dissertation, University of Chicago, Chicago, Ill., 1965.

Florida State University