MATH. SCAND. 20 (1967), 240–244

SOME APPLICATIONS OF THE HILFSSATZ VON DEDEKIND-MERTENS

ROBERT W. GILMER, JR.

Recently Arnold [1] has proved the following result:

Let R be a commutative ring containing a regular element, and let T be the total quotient ring of R. If $f,g \in T[X_1,\ldots,X_n]$ and if A, B, and C denote the fractional ideals of R generated by the coefficients of f, g, and fg, respectively, then there is a positive integer k such that $A^{k+1}B = A^kC$.

Arnold's theorem represents a broad generalization of a result due originally to Dedekind [4] and Mertens [13], proved in case R is an integral domain with identity and $n=1$. This result Krull refers to in [9, p. 128] as the *Hilfssatz von Dedekind–Mertens*. A form of the Hilfssatz von Dedekind–Mertens is proved by Prüfer [15, p. 24].

We present here some applications of the Dedekind–Mertens Lemma to the important case when R is a Prüfer domain, i.e., an integral domain D with identity such that each nonzero finitely generated ideal of D is invertible. The study of such domains originated with Prüfer's paper [15] and Krull developed some important aspects of the theory of Prüfer domains (called *Multiplikationsringe* by Krull) in [11]. In recent years renewed interest in the structure of such domains has been evident. For example, the papers of Jensen [8], Gilmer [5], Butts and Smith [3], and Ohm [14] contain basic results concerning the ideal theory of Prüfer domains. In a Prüfer domain the equality $A^{k+1}B = A^kC$ in the statement of Arnold's result implies that $AB = C$, since A^k is an invertible fractional ideal of R, and hence is a cancellation ideal. (The ideal Q of the commutative ring S is a *cancellation ideal* if there do not exist distinct ideals Q_1, Q_2 of S such that $QQ_1 = QQ_2$.)

In stating Theorem 1, we use this notation: D denotes an integral domain with identity having quotient field K. For $f \in K[X]$, A_f denotes the fractional ideal of D generated by the coefficients of f. We have already observed that $A_{fg} = A_f A_g$ for any $f,g \in K[X]$ in case D is a Prüfer domain. Theorem 1 establishes the converse.

Received December 13, 1966.

THEOREM 1. *If* $A_f A_g = A_{fg}$ *for any* $f,g \in K[X]$, *then* D *is a Prüfer domain.*

PROOF. By a result due to Prüfer, it suffices to prove that each nonzero fractional ideal of D with a basis of two elements is invertible [15, p. 7]]. Thus if a,b are nonzero elements of K, the equality $(aX-b)(aX+b)=a^2X^2-b^2$ implies that $(a,-b)(a,b)=(a^2,-b^2)$. Consequently, $ab \in (a^2,b^2)$. A result due to Butts and Smith [3, Prop. 3.9] then shows that (a,b) *is invertible if* D *is integrally closed.* (The method of proof of this result essentially goes back to Prüfer [15]. In Theorem 4.3 of [7], Gilmer proves a generalization of Butts and Smith's result.)

We complete the proof by establishing integral closure of D. Thus if $c \in K$ and if c is integral over D, there is a monic polynomial $f(X) \in D[X]$ such that $f(c)=0$. In $K[X]$ we have $f(X)=(X-c)g(X)$, where $g(X)$ is necessarily monic. The equality $A_f = A_{X-c}A_g$ then implies: $D=(1,c)A_g$, and since g is monic, $c \in (1,c)A_g$. Therefore, $c \in D$, D is integrally closed, and our proof is complete.

REMARK. Theorem 1 implies that if $A_{fg}=A_fA_g$ for any $f,g \in K[X]$, then the corresponding equality also holds for any $f,g \in K[X_1,\ldots,X_n]$. That this is true also follows as a corollary to this elementary result, proved in [1]: If S is a commutative ring and if $f,g \in S[X_1,\ldots,X_n]$, $n \geqq 2$, then there exist $f_1,g_1 \in S[X_1,\ldots,X_{n-1}]$ such that f and f_1, g and g_1, and fg and f_1g_1 have the same sets of coefficients.

The applications of Theorem 1 and its converse which we shall consider here concern ideal theoretic properties of a Prüfer domain under integral extensions. We introduce some notation which we use throughout the remainder of this paper. D denotes a Prüfer domain, K is the quotient field of D, and p is the characteristic exponent of K (that is, $p=1$ if K has characteristic 0; otherwise, p is the characteristic of K [2, p. 71]). L denotes a finite normal extension of K of degree n over K, and G denotes the Galois group of L/K. The order of G is equal to r, the separable degree of L/K, and $n=rp^k$ where p^k is the degree of inseparability of L/K. If $\bar{D}$ is the integral closure of D in L, $\bar{D}$ is a Prüfer domain [15, p. 22], and $\bar{D}$ is stable under G; that is, $\sigma(\bar{D})=\bar{D}$ for each $\sigma \in G$. Hence we may consider G as a group of automorphisms acting on $\bar{D}$. Following the terminology used in classical algebraic number theory [12, p. 62] we define, for any ideal A of $\bar{D}$, the *norm of* A, denoted by $N(A)$, to be

$$N(A) = [A^{(1)}A^{(2)}\ldots A^{(r)}]^{p^k},$$

where $G=\{\sigma_1=I,\sigma_2,\ldots,\sigma_r\}$ and where $A^{(i)}=\sigma_i(A)$; here I denotes the identity of G. Also, if $g \in L[X]$, A_g denotes the fractional ideal of $\bar{D}$

generated by the coefficients of g. (In algebraic number theory, A_g is called the *content* of g. A well-known result from algebraic number theory states that if L is a finite algebraic number field and if D is the ring of rational integers, then the content of the product of two polynomials over $\bar{D}$ is the product of the contents of the two polynomials [12, p. 68].)

Using this notation and terminology, we state and prove:

THEOREM 2. *If A is an ideal of $\bar{D}$, $N(A)$ has a basis consisting of elements of D. That is, $N(A)$ is the extension of an ideal of D.*

PROOF. We first consider the case when $A=(b_0, b_1, \ldots, b_s)$ is finitely generated. If for each i between 1 and r,

$$f^{(i)} = \sum_{j=0}^{s} \sigma_i(b_j) X^j ,$$

then $A^{(i)} = A_{f^{(i)}}$ for each i, so that

$$A^{(1)} \ldots A^{(r)} = A_{f^{(1)}} \ldots A_{f^{(r)}} = A_{f^{(1)} \ldots f^{(r)}} ,$$

the last equality holding because $\bar{D}$ is Prüfer. However, the coefficients of

$$f = f^{(1)} \ldots f^{(r)}$$

are left fixed by each element of G, and hence these coefficients are purely inseparable over K. It follows that $f^{p^k} \in D[X]$. But

$$N(A) = [A_f]^{p^k} = A_{f^{p^k}} ,$$

so that $N(A)$ has a basis consisting of elements of D as we wished to show.

In case A is not finitely generated, we consider the family $\{B_\lambda\}_{\lambda \in \Lambda}$ of finitely generated ideals of $\bar{D}$ contained in A. $\{B_\lambda\}$ is a directed set under $\subseteq$ and $A = \bigcup_{\lambda \in \Lambda} B_\lambda$. Further, the definition of $N(A) = [A^{(1)} \ldots A^{(r)}]^{p^k}$ as the set of all finite sums of products $x_1 x_2 \ldots x_{rp^k}$ of rp^k elements, p^k from each $A^{(i)}$, implies that each element of $N(A)$ is in $N(B_\lambda)$ for some $\lambda \in \Lambda$. Hence $N(A) = \bigcup_{\lambda \in \Lambda} N(B_\lambda)$, and $N(A)$ has a basis consisting of elements of D since $N(B_\lambda)$ has this property for each $\lambda \in \Lambda$.

COROLLARY 1. *If A is an ideal of $\bar{D}$ which is stable under G, then A^n has a basis consisting of elements of D.*

PROOF. Since A is stable under G, $A = A^{(1)} = \ldots = A^{(r)}$. Hence $N(A) = (A^r)^{p^k} = A^n$, and Corollary 1 follows from Theorem 2.

COROLLARY 2. *If B is an ideal of D which is equal to its own radical, and if A is the radical of $B\bar{D}$, then $A^n \subseteq B\bar{D}$.*

PROOF. It is clear that $B\bar{D}$ is stable under G, and this implies that A is also stable under G, for if $x \in A$ and if $x^m \in B\bar{D}$, then for any $\sigma \in G$,

$$\sigma(x^m) = [\sigma(x)]^m \in B\bar{D} \quad \text{so that} \quad \sigma(x) \in A;$$

hence $\sigma(A) \subseteq A$ and $\sigma^{-1}(A) \subseteq A$, and consequently,

$$A = \sigma(A).$$

Corollary 1 then implies that A^n is the extension to $\bar{D}$ of an ideal of D; in particular, $A^n = (A^n \cap D)\bar{D}$. Each element of A^n is in the radical of $B\bar{D}$, so that each element of $A^n \cap D$ is in the radical of $B\bar{D} \cap D$. But a result due to Krull [11, p. 752] shows that

$$(\sqrt{B\bar{D}}) \cap D = \sqrt{B} = B.$$

It follows that $A^n \cap D \subseteq B$ so that

$$A^n = (A^n \cap D)\bar{D} \subseteq B\bar{D}$$

as we wished to show.

COROLLARY 3. *If P is prime in D, the set of prime ideals of $\bar{D}$ lying over P is finite. If this set is $\{P_1, \ldots P_t\}$, then*

$$\left[\bigcap_{i=1}^{t} P_i\right]^n \subseteq P\bar{D}.$$

PROOF. By a theorem due to Krull, [11, p. 752], the primes of $\bar{D}$ lying over P are conjugate under elements of G. Hence the number of such primes is finite and is $\leqq r$. Since D is integrally closed, $\{P_1, \ldots P_t\}$ is the set of minimal primes of $P\bar{D}$ [11, p. 755], so that

$$P_1 \cap \ldots \cap P_t = \sqrt{P\bar{D}}.$$

From Corollary 2, it follows that $[\bigcap_{i=1}^t P_i]^n \subseteq P\bar{D}$.

REMARK. In the notation of Corollary 3, there are no containment relations among the P_i's since $\bar{D}$ is integral over D. But since $\bar{D}$ is Prüfer, this implies that the P_i's are pairwise comaximal. Hence

$$\bigcap_{i=1}^{t} P_i = \prod_{i=1}^{t} P_i.$$

The analogues of Corollaries 2, 3 are meaningful without the assumption that L is normal over K. We prove these analogues in Theorem 4.

THEOREM 4. *Let D be a Prüfer domain with quotient field K, let L_0 be a finite algebraic extension of K, and let D_0 be the integral closure of D in L_0. Let L be a normal closure of L_0/K and let $n = [L:K]$.*

(a) *If B is an ideal of D such that $B = \sqrt{B}$, and if $A_0 = \sqrt{BD_0}$, then $A_0{}^n \subseteq BD_0$.*

(b) *If P is prime in D, the set $\{P_i\}_{i=1}^t$ of prime ideals of D_0 lying over P is finite, and*

$$\left[\bigcap_{i=1}^{t} P_i\right]^n = \left[\prod_{i=1}^{t} P_i\right]^n \subseteqq PD_0 .$$

PROOF. (a): Let $A=\sqrt{B\bar{D}}$, where $\bar{D}$ is the integral closure of D in L. Then clearly $A_0 \subseteqq A$, and by Corollary 2, $A^n \subseteqq B\bar{D}$. Hence $A_0{}^n \subseteqq B\bar{D} \cap D_0$. But Corollary 2 of [6] shows that $B\bar{D} \cap D_0 = BD_0$.

(b) Since there are only finitely many primes of $\bar{D}$ lying over P and since each prime of D_0 lying over P is the contraction to D_0 of a prime ideal of $\bar{D}$ which lies over P, there are only finitely many primes of D_0 lying over P. Having made this observation, the proof of Theorem 4(b) is the same as the proof of Corollary 3 if this change is made in the proof of Corollary 3: replace "Corollary 2" by "Theorem 4(a)".

ADDED IN PROOF. After an abstract of this paper appeared in *Notices of the American Mathematical Society*, Professor Irving Kaplansky informed the author that Hwa Tsang proved Theorem 1 in her thesis. Hwa Tsang has not submitted her results for publication.

REFERENCES

1. J. T. Arnold and R. W. Gilmer, Jr., *On the lemma of Dedekind–Mertens*, submitted for publication.
2. N. Bourbaki, *Algèbre*, Chapitre 4–5 (Act. Sci. Ind. 1102), Paris, 1950.
3. H. S. Butts and W. W. Smith, *Prüfer rings*, Math. Z. 95 (1967), 196–211.
4. R. Dedekind, *Über einen arithmetischen Satz von Gauss*, Mitt. Deutsch. Math. Ges. Prag (1892), 1–11.
5. R. W. Gilmer, Jr., *Overrings of Prüfer domains*, J. Algebra 4 (1966), 331–340.
6. R. W. Gilmer, Jr., *Contracted ideals with respect to integral extensions*, Duke Math. J. (to appear).
7. R. W. Gilmer, Jr., *On a condition of Ohm's for integral domains*, submitted for publication.
8. Chr. U. Jensen, *On characterizations of Prüfer rings*, Math. Scand. 13 (1963), 90–98.
9. W. Krull, *Idealtheorie*, Berlin, 1935.
10. W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche*, Math. Z., 41 (1936), 545–577.
11. W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche* III, Math. Z. 42 (1937), 745–773.
12. H. B. Mann, *Introduction to algebraic number theory*, Columbus, 1955.
13. F. Mertens, *Über einen algebraischen Satz*, S.-B. Akad. Wiss. Wien Abtheilung II.a 101 (1892), 1560–1566.
14. J. Ohm, *Primary ideals in Prüfer domains*, Canad. J. Math. 18 (1966), 1024–1030.
15. H. Prüfer, *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, J. Reine Angew. Math. 168 (1932), 1–36.

FLORIDA STATE UNIVERSITY, TALLAHASSEE, U.S.A.