ON A CONDITION OF J. OHM FOR INTEGRAL DOMAINS[1]

ROBERT GILMER

1. Introduction. This paper originated mainly from results presented in a paper by J. Ohm (**13**), and, to a lesser degree, from results of Gilmer in (**3**). Ohm's paper is concerned with the validity of the equation $(x, y)^n = (x^n, y^n)$ for each pair of elements x, y of an integral domain D with identity. If D is a Prüfer domain,[2] the above equation is valid for all $x, y \in D$ (**7**, p. 244). Butts and Smith have shown (**2**) that if $(x, y)^2 = (x^2, y^2)$ for all x, y of the integrally closed domain D, then D is a Prüfer domain. Ohm, in (**13**), was concerned with the following question: Suppose $(x, y)^n = (x^n, y^n)$ for each $x, y \in D$, an integral domain with identity, and for each positive integer n; must D be integrally closed? Example 3.6 of (**13**) shows that the answer to this question is negative.

We present in this paper results in the area just discussed, some of which are generalizations of theorems in (**13**) and (**2**). All rings considered in this paper are assumed to be commutative and to contain an identity.

2. Some terminology. Suppose R is a ring. If S is a subset of R, (S) denotes the ideal of R generated by S. If n is a positive integer, we say R *has property* (n) provided $(x, y)^n = (x^n, y^n)$ for each $x, y \in R$; this is the terminology of Ohm in (**13**). We say R *has property* (n)* if for $x, y \in R$, $x^{n-1}y$ and xy^{n-1} are in (x^n, y^n). It is clear that property (n) implies property (n)*. We say R *has property* (n)′ if, from $x^n \in A^n$, it follows that $x \in A$ for any element $x \in R$ and any ideal A of R. Property (n)′ arises naturally in (**3**), where Gilmer proved (Theorem 5) that if A is an ideal of the integrally closed domain D having quotient field K and if $\bar{D}$ is the integral closure of D in L, an n-dimensional extension field of K, then for $x \in A\bar{D} \cap D$, $x^n \in A^n$.

If S is a unitary overring of R, we say that R *has property* (n) *with respect to* S provided the system of equations

$$(2.1)\qquad \begin{aligned} \xi &= a_1\xi^n + b_1 \\ \xi^2 &= a_2\xi^n + b_2 \\ &\vdots \\ \xi^{n-1} &= a_{n-1}\xi^n + b_{n-1} \end{aligned}$$

Received December 7, 1966.

[1]The author was supported during the writing of this paper by Alfred P. Sloan Foundation.

[2]An integral domain D is Prüfer if each finitely generated ideal of D is invertible. Equivalently, D_P is a valuation ring for each prime ideal P of D (**9**, p. 554). Properties of Prüfer domains may be found in (**1**, p. 93; **7**; **8**; **2**).

has a solution $\{a_1, b_1, \ldots, a_{n-1}, b_{n-1}\}$ in R for any $\xi \in S$. Again, this is Ohm's terminology. We say that R *has property* (n)* *with respect to* S provided, for each element ξ of S, there exist $a_1, b_1, a_{n-1}, b_{n-1} \in R$ such that

$$\xi = a_1\xi^n + b_1,$$
$$\xi^{n-1} = a_{n-1}\xi^n + b_{n-1}.$$

If R has property (n) with respect to S, then R has property (n)* with respect to S. The converse holds when $n = 2$ or 3. Ohm showed in (**13**) that if R is a domain having quotient field S, then R has property (n) if and only if R has property (n) with respect to S. In exactly the same way we obtain the following lemma.

LEMMA 2.1. *If R is a domain having quotient field S, then R has property* (n)* *if and only if R has property* (n)* *with respect to S.*

3. The equality $(x_1, x_2, \ldots, x_m)^n = (x_1^n, \ldots, x_m^n)$. If A is an ideal of the ring R, we say A is a *cancellation ideal* if from $AB = AC$, it follows that $B = C$; here B and C denote ideals of R. If A is invertible, A is a cancellation ideal. Products of cancellation ideals are again cancellation ideals; in particular, if A is a cancellation ideal and n is a positive integer, then A^n is a cancellation ideal.

LEMMA 3.1. *If $A = (a_1, \ldots, a_m)$ is a finitely generated cancellation ideal of the ring R, then for any positive integer n, $A^n = (a_1^n, \ldots, a_m^n)$.*

Proof. The ideal A^{mn} is generated by all products $a_1^{e_1} \ldots a_m^{e_m}$ such that $e_1 + \ldots + e_m = mn$, and, in each such product, at least one e_i must be $\geqq n$. Hence

$$\begin{aligned} A^{mn} &= A^n \cdot A^{(m-1)n} = (\{a_1^{e_1} \ldots a_m^{e_m} \mid \textstyle\sum_{j=1}^m e_j = mn\}) \\ &= (a_1^n, \ldots, a_m^n)(\{a_1^{f_1} \ldots a_m^{f_m} \mid \textstyle\sum_{j=1}^m f_j = (m-1)n\}) \\ &= (a_1^n, \ldots, a_m^n)A^{(m-1)n}, \end{aligned}$$

and because $A^{(m-1)n}$ is a cancellation ideal, it follows that $A^n = (a_1^n, \ldots, a_m^n)$.

From Lemma 3.1 it follows that if R is a ring in which each finitely generated ideal is a cancellation ideal, then R has property (n) for all n. But a ring in which each finitely generated ideal is a cancellation ideal is an integral domain, and is, in fact, a Prüfer domain. This result appeared as Corollary 1 of (**4**), but was originally due to H. S. Butts.

LEMMA 3.2. *Let n be a fixed positive integer. In the ring R,* (a) *and* (b) *are equivalent.*

(a) *If $\{r_1, \ldots, r_m\}$ is any finite subset of R, $(r_1, \ldots, r_m)^n = (r_1^n, \ldots, r_m^n)$.*
(b) *If S is any non-empty subset of R, $(S)^n = (\{s^n, \mid s \in S\})$.*

Either property implies property (n) *holds in R, and if R has property* (k) *for each positive integer $k \leqq n$, then* (a) *holds in R.*

https://doi.org/10.4153/CJM-1968-095-2 Published online by Cambridge University Press

Proof. We only prove that if R has property (k) for each positive integer $k \leqq n$, then (a) holds in R. The other assertions of the lemma are clear. Hence, if $\{r_1, \ldots, r_m\}$ is a finite subset of R, we need only show that

$$(r_1, \ldots, r_m)^n = (r_1^n, \ldots, r_m^n).$$

For this purpose, it suffices to show that $r_1^{e_1} \ldots r_m^{e_m} \in (r_1^n, \ldots, r_m^n)$ for any finite sequence $e_1, \ldots, e_m$ of non-negative integers with sum n. Thus

$$r_1^{e_1} r_2^{e_2} \in (r_1^{e_1+e_2}, r_2^{e_1+e_2})$$

since R has property $(e_1 + e_2)$. If we have shown that

$$r_1^{e_1} \ldots r_j^{e_j} \in (r_1^{e_1+\ldots+e_j}, \ldots, r_j^{e_1+\ldots+e_j}),$$

where $j < m$, then

$$r_1^{e_1} \ldots r_j^{e_j} r_{j+1}^{e_{j+1}} \in (r_1^{e_1+\ldots+e_j} r_{j+1}^{e_{j+1}}, \ldots \; r_j^{e_1+\ldots+e_j} r_{j+1}^{e_{j+1}})$$
$$\subseteq (r_1^{e_1+\ldots+e_{j+1}}, \ldots, r_{j+1}^{e_1+\ldots+e_{j+1}}),$$

the last containment following since R has property $(e_1 + \ldots + e_{j+1})$. By induction, it follows that $r_1^{e_1} \ldots r_m^{e_m} \in (r_1^n, \ldots, r_m^n)$, as required.

4. Property (n)*. If S is a unitary overring of the ring R and if n is a positive integer, an element s of S is said to be *n-integral over R* provided s is a root of a monic polynomial of degree n having coefficients in R. R is *n-integrally closed in S* if each element of S, n-integral over R, is in R. In case S is the total quotient ring of R, if R is n-integrally closed in S, we simply say that *R is n-integrally closed*. We present in this section a generalization (Corollary 4.4) to Corollary 3.10 of (**2**), using the notion of n-integrally closed.

Remark. If the element s is n-integral over R, then s is m-integral over R for any $m \geqq n$. Hence, if R is n-integrally closed, then R is k-integrally closed for any $k \leqq n$.

LEMMA 4.1. *If the domain R is n-integrally-closed, then for any multiplicative system N in R, R_N is n-integrally closed. If $\{M_\lambda\}$ is the set of maximal ideals of R and if R_{M_λ} is n-integrally closed for each λ, then R is n-integrally closed.*

Proof. The technique required for the proof of the first assertion is well known (cf. **15**, p. 262), and the second statement follows from the fact that $R = \bigcap_\lambda R_{M_\lambda}$ (**16**, p. 94).

LEMMA 4.2. *If B is a finitely generated ideal of the domain D and if $\{M_\lambda\}$ is the collection of maximal ideals of D, then B is invertible in D if and only if BD_{M_λ} is invertible in D_{M_λ} for each λ.*

Proof. See (**11**, p. 233).

Remark. The assumption that B is finitely generated is necessary for the validity of Lemma 4.2. For example, there is an integral domain J such that J_M is a rank one discrete valuation ring for each maximal ideal M of J, and such that J is not a Dedekind domain (**12**, p. 426; **5**, p. 814). If A is a non-zero ideal of J, it is true that AJ_M is invertible for each maximal ideal M of J. But there is a non-zero ideal A of J such that A is not invertible (**15**, p. 275). In the particular example given by Nakano of such a J it is, in fact, true that the only invertible ideals of J are non-zero principal ideals. In the proof of Lemma 4.2, the equality $bD_{M_\lambda} : BD_{M_\lambda} = [(b) : B]D_{M_\lambda}$ depends upon the fact that B is finitely generated.

Remark. Invertible ideals of a quasi-local domain are principal (**11**, p. 233). Hence, Lemma 4.2 can be stated as follows.

If B is a finitely generated ideal of the domain D and if $\{M_\alpha\}$ is the collection of maximal ideals of D containing B, then B is invertible in D if and only if BD_{M_α} is principal in D_{M_α} for each α.

THEOREM 4.3. *Suppose n is an integer greater than one and D is an n-integrally closed domain. If a and b are non-zero elements of D such that $a^{n-1}b$ and ab^{n-1} are in (a^n, b^n), then (a, b) is invertible.*

Proof. We first assume that D is quasi-local with maximal ideal M. We let $a^{n-1}b = ra^n + sb^n$ and $ab^{n-1} = ua^n + vb^n$, where $r, s, u, v \in D$. Multiplying the first equation by r^{n-1}/b^n, we obtain $(ra/b)^n - (ra/b)^{n-1} + r^{n-1}s = 0$, so that ra/b is n-integral over D, and hence is in D. Since $1 = (ra/b) + s(b/a)^{n-1}$, we conclude that either ra/b or $1 - (ra/b) = s(b/a)^{n-1}$ is a unit of D. If ra/b is a unit of D, then $(a, b) = (a)$ so that (a, b) is invertible. We assume that $s(b/a)^{n-1}$ is a unit of D.

From the equation $ab^{n-1} = ua^n + vb^n$ we conclude, in like manner, that vb/a is n-integral over D, and hence is in D; vb/a or $1 - (vb/a) = u(a/b)^{n-1}$ is a unit of D. If vb/a is a unit, then $(a, b) = (b)$ is invertible. We therefore assume that $u(a/b)^{n-1}$ is a unit of D. In this case, $s(b/a)^{n-1} \cdot u(a/b)^{n-1} = su$ is a unit of D; hence, s and u are units of D. The equality

$$(b/a)^n - s^{-1}(b/a) + rs^{-1} = 0$$

then shows that b/a is n-integral over D so that $(b/a) \in D$ and $(a, b) = (a)$ is invertible.

In case D is not quasi-local, we consider any maximal ideal M_λ of D. By Lemma 4.1, D_{M_λ} is n-integrally closed, and $a^{n-1}b, ab^{n-1} \in (a^n, b^n)$ imply that $a^{n-1}b, ab^{n-1} \in (a^n, b^n)D_{M_\lambda}$. By the proof just given, it is implied that $(a, b)D_{M_\lambda}$ is invertible. Because M_λ is an arbitrary maximal ideal of D, Lemma 4.2 then shows that (a, b) is an invertible ideal of D.

In (**14**, p. 6), Prüfer showed that if each non-zero ideal of a domain D with a basis of two elements is invertible, then each non-zero finitely generated ideal of D is invertible. From this and from Theorem 4.3, Corollary 4.4 then follows.

Corollary 4.4. *If the domain D is n-integrally closed and has property* (n)*, *where n is a fixed positive integer >1, then D is a Prüfer domain.*

Corollary 4.5 *Let D be a domain, $\bar{D}$ its integral closure, and n an integer >1. If a and b are non-zero elements of D such that $a^{n-1}b$ and ab^{n-1} are in (a^n, b^n), then $(a, b)\bar{D}$ is invertible in $\bar{D}$.*

Corollary 4.6. *If the domain D with quotient field K has property* (n)*, *where $n > 1$, then any n-integrally closed domain between D and K is Prüfer. In particular, the integral closure of D is Prüfer.*

Proof. Lemma 2.1 shows that if D has property (n)*, then any domain between D and K has property (n)*. Hence, Corollary 4.6 follows from Corollary 4.4.

Remark. Corollary 4.4 generalizes Corollary 3.10 of (**2**). Our next result, Theorem 4.7, is a generalization of Proposition 3.9 of (**2**) and is also a generalization of our Theorem 4.3.

Theorem 4.7. *Let n be an integer >1, and let R be a ring such that R is n-integrally closed. If a and b are elements of R such that a is regular and $a^{n-1}b \in (a^n, b^n)$, then (a, b) is invertible.*

Proof. We suppose $a^{n-1}b = ra^n + sb^n$, where $r, s \in R$. As shown in the proof of Theorem 4.3, sb/a is an element of the total quotient ring of R which is n-integral over R. Hence, $sb/a = s_1 \in R$. Thus $a^{n-1}b = ra^n + s_1ab^{n-1}$, and since a is regular in R, $a^{n-2}b = ra^{n-1} + s_1b^{n-1}$ so that $a^{n-2}b \in (a^{n-1}, b^{n-1})$. By the remark preceding Lemma 4.1, R is $(n-1)$-integrally closed. Therefore, the same method as was just used implies (if $n > 3$) $a^{n-3}b \in (a^{n-2}, b^{n-2})$. By induction, it follows that $ab \in (a^2, b^2)$. A proof by Butts and Smith (**2**) then shows that (a, b) is invertible in R.

Proposition 4.8. *If $\{M_\lambda\}$ is the set of maximal ideals of the domain D, then D has property* (n)* *if and only if each D_{M_λ} has property* (n)*.

Proof. Lemma 2.1 shows that if D has property (n)*, each D_{M_λ} has property (n)*. We suppose each D_{M_λ} has property (n)*, and we choose ξ in K, the quotient field of D. We wish to show that ξ and ξ^{n-1} belong to the D-submodule N of K generated by ξ^n and 1. The set A of elements d of D such that $d\xi \in N$ is an ideal of D. We need to show that $A = D$, and to do so, it suffices to show that $A \not\subseteq M_\lambda$ for any λ. Thus, for any λ, there are elements u_λ and v_λ of D_{M_λ} such that $\xi = u_\lambda\xi^n + v_\lambda$. There is an element d_λ of $D - M_\lambda$ such that $d_\lambda u_\lambda$ and $d_\lambda v_\lambda$ are in D; hence $d_\lambda\xi = (d_\lambda u_\lambda)\xi^n + (d_\lambda v_\lambda) \in N$ so that $d_\lambda \in A - M_\lambda$. This shows that $\xi \in N$. The proof that $\xi^{n-1} \in N$ is similar.

5. The properties (n)′, (n), (n)*, and integral closure.

We show here that for any integer $n > 1$, a Prüfer domain has property (n)′, and that a ring with property (n)′ has property (n). Since a domain with property (n)* is Prüfer if and only if it is n-integrally closed (Corollary 4.4), a domain with property (n)′ is also Prüfer if and only if it is n-integrally closed. We show (Example 5.7) that a domain having property (n)′ for all $n > 1$ need not be Prüfer, and we further investigate relations between the properties mentioned in the heading of this section.

If A is an ideal of a domain D, A is called a *valuation ideal* (**16**, p. 340) if there is a valuation ring V containing D as a subring and an ideal B of V such that $B \cap D = A$. If A is a valuation ideal, the valuation ring V may be taken to lie between D and its quotient field (**16**, p. 340).

LEMMA 5.1. *If the ideal A of the domain D is an intersection of valuation ideals of D, and if $x \in D$ is such that $x^n \in A^n$, where n is some positive integer, then $x \in A$.*

Proof. By assumption, there is a collection $\{A_\lambda\}$ of valuation ideals of D such that $A = \bigcap_\lambda A_\lambda$. For any such λ, $x^n \in A^n \subseteq A_\lambda{}^n$, so it suffices to observe that Lemma 5.1 is true when A is a valuation ideal. But this follows from Corollary 2.9 of (**7**).

Gilmer and Ohm in (**7**, p. 238) showed that among integral domains D, Prüfer domains are characterized by the property that each ideal of D is an intersection of valuation ideals. Corollary 5.2 follows from this fact and from Lemma 5.1.

COROLLARY 5.2. *If D is a Prüfer domain, D has property* (n)′ *for any positive integer n.*

Remark. If A is an ideal of a commutative ring R, each element x of A^n belongs to $A_x{}^n$ for some finitely generated ideal A_x contained in A. Hence, in order that R have property (n)′, it is sufficient that $x^n \in B^n$ should imply $x \in B$ for any element x of R and any finitely *generated ideal* B of R.

THEOREM 5.3. *If R is a ring having property* (n)′, *then for any non-empty subset S of R, $(S)^n = (\{s^n | s \in S\})$. Hence property* (n) *holds in R.*

Proof. By Lemma 3.2, it suffices to prove Theorem 5.3 when $S = \{s_1, \ldots, s_m\}$ is a finite subset of R. We need only show that if $i_1, \ldots, i_m$ are non-negative integers with sum n, then $s = s_1{}^{i_1} s_2{}^{i_2} \ldots s_m{}^{i_m} \in (s_1{}^n, \ldots, s_m{}^n)$. We observe that $s^n = (s_1{}^n)^{i_1} \ldots (s_m{}^n)^{i_m} \in (s_1{}^n, \ldots, s_m{}^n)^n$ so that $s \in (s_1{}^n, \ldots, s_m{}^n)$ since property (n)′ holds in R.

Propositions 1.6 and 1.7 of (**13**) provided Ohm with a method for constructing domains with property (n) for a given integer $n > 1$. We cite these results, and remark that these statements remain valid if *property* (n) is replaced throughout by property (n)*.

PROPOSITION 1.6. *If D' is a valuation ring between the domain D and its quotient field, D has property* (n) *if and only if D has property* (n) *with respect to D'.*

Proposition 1.7. *Let $R \subseteq R'$ be rings which have a common ideal A. Then R is integrally closed in R' if and only if R/A is integrally closed in R'/A, and R has property* (n) *with respect to R' if and only if R/A has property* (n) *with respect to R'/A.*

If V is a valuation ring of the form $K + A$, where K is a field and A is the maximal ideal of V, and if k is a subfield of K, then the domain $D = k + A$ has property (n) if and only if k has property (n) with respect to K. We show that this method for constructing a domain with property (n) always yields a domain with property (n)′. We first investigate the class of finitely generated ideals of such a domain D. We use the following notation. V is a valuation ring of the form $K + M$, where K is a field and M is the maximal ideal of V, v is a valuation associated with the valuation ring V, k is a subfield of K, and $D = k + M$.

Lemma 5.4. *If $x \in D - \{0\}$, xD contains each element y of V such that $v(y) > v(x)$. If A is a finitely generated ideal of D, say $A = \{a_1, \ldots, a_n\}D$, and if $t = \min\{v(a_i) \mid 1 \leqq i \leqq n\}$, then for any element b of A such that $v(b) = t$, A has a basis of the form $b, k_2b, \ldots, k_mb$ for some $k_2, \ldots, k_m \in K - k$. If $b \in D - \{0\}$, b not a unit, and if $k_2, \ldots, k_m \in K$, the ideal of D generated by $\{b, k_2b, \ldots, k_mb\}$ is $Wb + B$, where W is the k-subspace of K generated by $\{1, k_2, \ldots, k_m\}$ and B is the ideal of V consisting of all elements y such that $v(y) > t$.*

Proof. If $v(y) > v(x)$, then $y/x \in M \subseteq D$, therefore $y \in Mx \subseteq Dx$. Thus, if $A = \{a_1, \ldots, a_n\}D$ and if $t = \min\{v(a_i) \mid 1 \leqq i \leqq n\}$, then $A = \{a_1, \ldots, a_m\}D$, where $t = v(a_1) = \ldots = v(a_m) < v(a_j)$ for $m + 1 \leqq j \leqq n$. If $b = a_1$, then $v(a_i/b) = 0$ for $2 \leqq i \leqq m$. Hence, $a_i/b = k_i + m_i$ for some $k_i \in K$, $m_i \in M$. It follows that $a_i = k_ib + m_ib$ for each i. But $m_ib \in Db$ for $2 \leqq i \leqq m$ so that $A = \{b, k_2b + m_2b, \ldots, k_mb + m_mb\}D = \{b, k_2b, \ldots, k_mb\}D$.

It is clear that for any $b \in D$ with $v(b) \neq 0$, $\{b, k_2b, \ldots, k_mb\}D$ contains $Wb + B$, and $\{b, k_2b, \ldots, k_mb\} \subseteq Wb + b$. Hence, if $Wb + B$ is an ideal of D, then $Wb + B$ is the ideal generated by $\{b, k_2b, \ldots, k_mb\}$. To check that $Wb + B$ is an ideal of D is straightforward.

Lemma 5.5. *If k has property* (n) *with respect to K, then for S a subset of K linearly independent over k, $\{s^n \mid s \in S\}$ is linearly independent over k.*

Proof. It suffices to consider the case when $S = \{s_1, s_2, \ldots, s_m\}$ is finite. We first note that $\{1 = t_1, t_2, \ldots, t_m\}$ is linearly independent over k, where $t_i = s_i/s_1$ for each i between 1 and m. Thus, if $\sum_{i=1}^m a_it_i = 0$, where each $a_i \in k$, then $0 = s_1\sum_1^m a_it_i = \sum_1^m a_is_i$, so that $a_i = 0$ for each i. We show that $\{t_1^n = 1, t_2^n, \ldots, t_m^n\}$ is linearly independent over k. Because k has property (n) with respect to K, it is clear that each t_i belongs to the k-subspace $k\langle t_1^n, \ldots, t_m^n\rangle$ of K spanned by $\{t_1, \ldots, t_m\}$. Since $k\langle t_1, \ldots, t_m\rangle$ is m-dimensional, it follows that $k\langle t_1, \ldots, t_m\rangle = k\langle t_1^n, \ldots, t_m^n\rangle$ and that

$\{t_1^n, \ldots, t_m^n\}$ is linearly independent over k. We have already shown that this implies that $\{s_1^n t_1^n, \ldots, s_1^n t_m^n\} = \{s_1^n, \ldots, s_m^n\}$ is linearly independent over k.

THEOREM 5.6. *If k has property* (n) *with respect to K, then D has property* (n)$'$.

Proof. By the remark preceding Theorem 5.3, it suffices to prove, for B a finitely generated ideal of D and an element x of D such that $x^n \in B^n$, that $x \in B$. If $B = D$ or $B = (0)$, there is nothing to prove. Otherwise, Lemma 5.4 implies B has a basis of the form $\{b, k_2b, \ldots, k_mb\}$ for some finite subset $\{k_2, \ldots, k_m\}$ of K. If W is the k-subspace of K generated by $\{1, k_2, \ldots, k_m\}$, we may choose a basis S of W such that $1 \in S$ and $S \subseteq \{1, k_2, \ldots, k_m\}$. Therefore, we may assume $\{1, k_2, \ldots, k_m\}$ is linearly independent over k. Since k has property (n) with respect to K, D has property (n). Hence $B^n = \{b^n, k_2^nb^n, \ldots, k_m^nb^n\}D$. We have $x^n \in B^nV = (BV)^n$ and V is a valuation ring so that $x \in BV = bV$. It follows that $v(x) \geqq v(b)$. If $v(x) > v(b)$, Lemma 5.4 shows that $x \in bD \subseteq B$. If $v(x) = v(b)$, then $v(x/b) = 0$ so that $x/b = u + m$ for some non-zero element u of K and some element m of M. Hence $x = ub + mb$ and $x \equiv ub(B)$. Thus $x^n \equiv (ub)^n \equiv 0\ (B^n)$ and to show that $x \in B$, it suffices to show that $ub \in B$. Now, $B^n = \{b^n, k_2^nb^n, \ldots, k_m^nb^n\}D = Wb^n + C$, where W is the k-subspace of K generated by $\{1, k_2^n, \ldots, k_m^n\}$ and C is the ideal of V consisting of all elements having v-value greater than $v(b^n)$. Since $u^nb^n \in B^n$, we have $u^nb^n = yb^n + c$ for some $y \in W$ and some $c \in C$. Hence $c = (u^n - y)b^n$, implying, since $v(c) > v(b^n)$ and $u^n - y \in K$, that $c = u^n - y = 0$. Therefore, $u^n \in W$; $\{u^n, 1, k_2^n, \ldots, k_m^n\}$ are linearly dependent over k. By Lemma 5.5, $\{u, 1, k_2, \ldots, k_m\}$ are linearly dependent over k. Since $\{1, k_2, \ldots, k_m\}$ are linearly independent over k, we conclude that u depends linearly upon $\{1, k_2, \ldots, k_m\}$. Hence

$$ub \in kb + k(k_2b) + \ldots + k(k_mb) \subseteq B.$$

Example 5.7. In (**13**), Ohm constructed fields k and K such that k has property (n) with respect to K for each positive integer n, but such that k is not algebraically closed in K. If $V = K[[X]]$ is the ring of formal power series in X over K, then V is a rank one discrete valuation ring of the form $K + M$, where M is the maximal ideal of V. It then follows that the domain $D = k + M$ has property (n) for each positive integer n, but D is not integrally closed, hence is not Prüfer. Theorem 5.6 shows that D does, in fact, have property (n)$'$ for each positive integer n.

6. Property (n) **for field extensions.** Ohm's construction of domains having property (n), which we have outlined in § 5, gives rise to the following field-theoretic question: Suppose k is a subfield of the field K and n is a positive integer. Under what conditions does k have property (n) with respect to K? There are a few simple observations we can make in connection with this question. First, k has property (n) with respect to K if and only if k has property (n) with respect to $k(t)$ for each $t \in K$. Hence, we may restrict ourselves to the case when $K = k(t)$ is a simple extension of k, and, clearly, K/k must be algebraic if k is to have property (n) with respect to K. By definition, k has property (n) with respect to K if and only if for $\xi \in K - k$, there exist polynomials

$$
\begin{aligned}
f_1(X) &= a_1X^n - X + b_1 \\
f_2(X) &= a_2X^n - X^2 + b_2 \\
&\ \ \vdots \\
f_{n-1}(X) &= a_{n-1}X^n - X^{n-1} + b_{n-1}
\end{aligned}
$$

in $k[X]$ having ξ as a root. For $\xi \notin k$, $a_1 \neq 0$; therefore $[k(\xi) : k] \leqq n$. Hence, a necessary condition for k to have property (n) with respect to $k(t)$ is that $[k(t) : k] \leqq n$, and equality can hold only when $n = 2$.

A general investigation of the question as to when k has property (n) with respect to $k(t)$ has allowed us to realize that this question is too large for consideration in conjunction with this paper and we shall examine this problem separately in a forthcoming paper. We do consider, however, two special cases of the question here. The first case, when $n = 3$ and $[k(t):k]=2$, is mentioned here, since it is directly related to Corollary 3.4 of (**13**). In the second case, when $n = 5$ and $[k(t) : k] = 2$, a good insight into the nature of the question is given.

THEOREM 6.1. *If $k(t)$ is an extension field of the field k such that $[k(t):k] = 2$, then k has property "(3)" with respect to $k(t)$ if and only if each root of $X^2 + X + 1$ in $k(t)$ belongs to k.*

Proof. Suppose $X^2 + X + 1$ has a root θ in $k(t)$ such that $\theta \in k$. Then $X^2 + X + 1$ is the minimal polynomial of θ over k. If $\theta = v\theta^3 + u$ for some $u, v \in k$, then $\theta \notin k$ implies $v \neq 0$. Hence, θ is a root of $X^3 - aX + b$, where $a = v^{-1}$ and $b = uv^{-1}$ are in k. Therefore, $X^3 - aX + b$ is divisible by $X^2 + X + 1$ so that

$$X^3 - aX + b = (X - d)(X^2 + X + 1) = X^3 + (1 - d)X^2 + (1 - d)X - d$$

for some $d \in k$. Hence, $d - 1 = 0 = a$, a contradiction. It follows that if k has property "(3)" with respect to $k(t)$, then each root of $X^2 + X + 1$ in $k(t)$ is in k.

To prove the converse, it is sufficient to show that if $\xi \in k(t) - k$ and if $X^2 + aX + b$ is the minimal polynomial for ξ over k, then there are elements c and d of k such that $(X - c)(X^2 + aX + b) = X^3 + eX^2 + f$ and $(X - d)(X^2 + aX + b) = X^3 + gX + h$ for some $e, f, g, h \in K$. It is easy to check that the condition needed to assert the existence of such an element c or d is that $b \neq a^2$. Why is this condition fulfilled? If θ is a root of X^2+aX+a^2

over k, then θ/a is a root of $X^2 + X + 1$. Therefore, if $\theta \in k(t)$, then $\theta/a \in k(t)$, and, hence, $\theta/a \in k$ and $\theta \in k$. Thus, if $\xi \in k(t) - k$, the minimal polynomial for ξ over k does not have the form $X^2 + aX + a^2$.

THEOREM 6.2. *If $k(t)$ is an extension field of the field k such that $[k(t):k] = 2$, then k has property "(5)" with respect to $k(t)$ if and only if each root of $X^4 + 2X^3 + 4X^2 + 3X + 1$ in $k(t)$ belongs to k.*

Proof. By definition, k has property "(5)" with respect to $k(t)$ if and only if for each $\theta \in k(t) - k$, there exist polynomials

$$f_1(X) = a_1X^5 - X + b_1, \ldots, f_4(X) = a_4X^5 - X^4 + b_4$$

in $k[X]$ having θ as a root. If $X^2 + aX + b$ is the minimal polynomial for θ over k, we must therefore be able to find elements y_0, y_1, y_2, y_3 in k such that, in

$$(y_0 + y_1X + y_2X^2 + y_3X^3)(b + aX + X^2) = u_0 + u_1X + u_2X^2 + u_3X^3 + u_4X^4 + u_5X^5,$$

any three of $\{u_1, u_2, u_3, u_4\}$ may be zero, while the fourth is one. This is equivalent to the assertion that the system

$$\begin{aligned} ay_3 + y_2 \qquad\qquad\quad &= u_4 \\ by_3 + ay_2 + y_1 \qquad &= u_3 \\ by_2 + ay_1 + y_0 &= u_2 \\ by_1 + ay_0 &= u_1 \end{aligned}$$

has a solution when any three of u_4, u_3, u_2, u_1 are zero and the fourth is one. But this is equivalent to invertibility of the matrix

$$\begin{bmatrix} a & 1 & 0 & 0 \\ b & a & 1 & 0 \\ 0 & b & a & 1 \\ 0 & 0 & b & a \end{bmatrix}$$

which holds if and only if its determinant $a^4 - 3a^2b + b^2 \neq 0$. Since $b = -a\theta - \theta^2$ and

$$a^4 - 3a^2(-a\theta - \theta^2) + (-a\theta - \theta^2)^2 = \theta^4 + 2a\theta^3 + 4a^2\theta^2 + 3a^3\theta + a^4,$$

the following criterion is valid: *k has property "(5)" with respect to $k(t)$ if and only if* $\theta^4 + 2a\theta^3 + 4a^2\theta^2 + 3a^3\theta + a^4 \neq 0$ for each element $\theta \in k(t) - k$, *where a is the coefficient of X in the minimal polynomial for θ over k.* Hence, suppose each root of $f(X) = X^4 + 2X^3 + 4X^2 + 3X + 1$ in $k(t)$ is in k. If then $\theta \in k(t)$ and $a \in k$ are such that

$$\theta^4 + 2a\theta^3 + 4a^2\theta^2 + 3a^3\theta + a^4 = 0,$$

https://doi.org/10.4153/CJM-1968-095-2 Published online by Cambridge University Press

then if $a = 0$, $\theta^4 = 0$ so $\theta = 0$ and $\theta \in k$. If $a \neq 0$, then $\theta/a \in k(t)$ and is a root of $f(X)$. Thus, by assumption, $\theta/a \in k$ so that $\theta \in k$ also. It follows that if each root of $f(X)$ in $k(t)$ is in k, then k has property "(5)" with respect to $k(t)$.

To prove the converse, we examine more closely the polynomial $f(X)$. If P is the prime field of k, then $f(X) \in P[X]$. If s is an element of an extension field of P such that $s^2 = 3s - 1$, then $f(X) = (X^2 + X + s)(X^2 + X + 3-s)$ in $P(s)[X]$. Further, if θ is a root of $X^2 + X + s$ in an extension field of $P(s)$, $-1 - \theta$ is also a root of $X^2 + X + s$ and $2 - s + (5 - 2s)\theta$ and $s - 3 + (2s - 5)\theta$ are roots of $X^2 + X + 3 - s$. It follows that if $\theta_1 = \theta$ is one root of $f(X)$ in an extension field of P, then $\theta_2 = -1 - \theta$, $\theta_3 = 2 + \theta + \theta^2 + (5 + 2\theta + 2\theta^2)\theta = 2 + 6\theta + 3\theta^2 + 2\theta^3$, and $\theta_4 = -1 - \theta_3 = -3 - 6\theta - 3\theta^2 - 2\theta^3$ are also roots of $f(X)$ in $P(\theta)$. Hence the field $P(\theta)/P$ is normal. We observe that if $\xi = \theta_1\theta_3$, then $\theta = -\xi - \xi^3$ and if $\sigma = \theta_1 + \theta_4$, then $\theta = -4 - 5\sigma - 3\sigma^2 - \sigma^3$. It then follows that $P(\theta_1) = P(\theta_1 + \theta_4) = P(\theta_1\theta_3)$. Therefore, the factorization of $f(X)$ in $F[X]$ for any field F containing P is either into linear factors, or $f(X)$ is irreducible, or

$$f(X) = (X^2 + X + g)(X^2 + X + h) \quad \text{for some } g, h \in F.$$

We return to our proof of Theorem 6.2. We suppose there is a root θ of $f(X)$ in $k(t)$, not in k. Then $k(\theta) = k(t)$ and the minimal polynomial for θ over k has the form $X^2 + X + g$ for some $g \in k$. Hence, the coefficient, a, of X in the minimal polynomial for θ over k is 1 so that

$$\theta^4 + 2a\theta^3 + 4a^2\theta^2 + 3a^3\theta + a^4 = f(\theta) = 0.$$

Hence, k does not have property "(5)" with respect to $k(t)$ according to the criterion developed earlier in our proof.

Remark. In considering conditions under which k has property (n) with respect to $k(t)$ for values of n greater than 5, more sophisticated techniques are required than those employed in the proof of Theorem 6.2, even when $[k(t) : k] = 2$. However, it is fairly easy to establish the following: When $[k(t) : k] = 2$, then for any integer $n \geqq 3$, there is a monic polynomial $f_n(X) \in P[X]$, where P is the prime field of k, of degree $n - 1$, such that if each root of $f_n(X)$ in $k(t)$ belongs to k, then k has property (n) with respect to $k(t)$. Combining this fact with Ohm's Theorem 2.1 in (**13**), we have the following: If the field k has characteristic 2 and contains an algebraic closure of its prime field, then k has property (n) with respect $k(t)$ for each positive integer n, where $k(t)$ is any separable quadratic extension of k.

The polynomials $X^2 + X + 1$ and $X^4 + 2X^3 + 4X^2 + 3X + 1$ mentioned in Theorems 6.1 and 6.2 are not unique. For example, $X^4 - 2X^3 + 4X^2 - 3X + 1$ is also suitable when $n = 5$ since its roots are the additive inverses of the roots of $X^4 + 2X^3 + 4X^2 + 3X + 1$.

7. Another construction of domains having property (n)**.** We give a method of constructing domains having property (n) which are not integrally closed; the method is quite different from that used by Ohm in (**13**).

https://doi.org/10.4153/CJM-1968-095-2 Published online by Cambridge University Press

THEOREM 7.1. *Suppose that V_1 and V_2 are independent valuation rings having a common quotient field L, that K is a common subfield of V_1 and V_2, and that $V_i = K + M_i$, where M_i is the maximal ideal of V_i. Then $D = K + (M_1 \cap M_2)$ is a quasi-local domain with quotient field L, and D is not integrally closed. If n is a positive integer, D has property* (n) *if and only if the mapping $x \to x^n$ of K into K is one-to-one.*

Proof. Gilmer and Heinzer showed (see **6**) that D is a quasi-local domain with quotient field L having integral closure $V_1 \cap V_2 \supset D$. (The assumption that V_1 and V_2 are independent is not needed for this part of the theorem. The only requirement for the validity of the first statement of the conclusion is that $V_1 \not\subseteq V_2$ and $V_2 \not\subseteq V_1$.)

To establish our conclusion concerning property (n), we first suppose that $x \to x^n$ is one-to-one. To show that D has property (n), it suffices to show that D has property (n) with respect to V_1. Thus, we take $\xi \in V_1 - \{0\}$ and an integer i such that $1 \leqq i \leqq n - 1$. We show that there is an element a of D such that $\xi^i - a\xi^n \in D$. Let v_i be a valuation associated with the valuation ring V_i. We first consider the case when $v_1(\xi) > 0$. Then, if $v_2(\xi) > 0$, $\xi \in M_1 \cap M_2 \in D$ and we may choose $a = 0$. If $v_2(\xi) = -\alpha < 0$, we choose, by the approximation theorem for independent valuations (**16**, p. 47), an element a of L such that $v_1(a) > 0$ and $v_2(a - (\xi^{-1})^{n-i}) > -v_2(\xi^n)$. Since $v_2((\xi^{-1})^{n-i}) = (n - i)\alpha < n\alpha = -v_2(\xi^n)$, it follows that

$$v_2(a) = (n - i)\alpha > 0.$$

Hence $a \in M_1 \cap M_2 \subseteq D$. Further,

$$v_2(\xi^i - a\xi^n) = v_2((\xi^{-1})^{n-i} - a) + v_2(\xi^n) > 0$$

by choice of a, and $v_1(\xi^i - a\xi^n) > 0$ since $v_1(\xi)$, $v_1(a) > 0$. It follows that $\xi^i - a\xi^n \in D$, and our proof is complete for $v_1(\xi) > 0$ and $v_2(\xi) \neq 0$. If $v_1(\xi) > 0$ and $v_2(\xi) = 0$, we may write $\xi = u + m$, where $u \in K - \{0\}$ and $m \in M_2$. By the approximation theorem, there is an element a in L such that $v_1(a - (u^{-1})^{n-i}) > 0$ and $v_2(a - (u^{-1})^{n-i}) > 0$. Hence

$$a = (u^{-1})^{n-i} + [a - (u^{-1})^{n-i}] \in K + (M_1 \cap M_2) = D.$$

It follows that $v_1(\xi^i - a\xi^n) > 0$ since $v_1(\xi) > 0$ and $v_1(a) = 0$. Further, if $a - (u^{-1})^{n-i} = h$, then

$$\xi^i - a\xi^n = (u + m)^i - [(u^{-1})^{n-i} + h](u + m)^n \equiv u^i - (u^{-1})^{n-i}(u)^n \equiv 0 \ (M_2)$$

so that $\xi^i - a\xi^n \in M_2$. Consequently, $\xi^i - a\xi^n \in M_1 \cap M_2$, and our proof is complete in the case when $v_1(\xi) > 0$.

The case when $v_1(\xi) = 0$ and $v_2(\xi) > 0$ is similar to the case just considered, and will be omitted. If $v_1(\xi) = 0$ and $v_2(\xi) < 0$, then $v_1(\xi^{-1}) = 0$ and $v_2(\xi^{-1}) > 0$, so that our second case implies the existence of $a, b \in D$ such that $(\xi^{-1})^{n-i} - a(\xi^{-1})^n = b$. Multiplying by ξ^n, we therefore have: $\xi^i - b\xi^n = a \in D$.

Therefore, we may consider the case when $v_1(\xi) = v_2(\xi) = 0$. In this case we write $\xi = u_1 + m_2 = u_2 + m_2$, where $u_1, u_2 \in K$ and $m_i \in M_i$. If $u_1 = u_2$, then $m_1 - m_2 \in M_1 \cap M_2$, $\xi \in D$, and we take $a = 0$. If $u_1 \neq u_2$, then $u_1^n \neq u_2^n$ by our hypothesis. Therefore, $a = (u_1^i - u_2^i)/(u_1^n - u_2^n) \in K$. And modulo M_j, for $j = 1$ or 2, we have

$$\xi^i - a\xi^n \equiv (u_1^n u_2^i - u_1^i u_2^n)/(u_1^n - u_2^n) = q \in K.$$

Thus $\xi^i - a\xi^n - q \in M_1 \cap M_2$ and $\xi^i - a\xi^n \in D$ as required. We have therefore shown that if $x \to x^n$ is one-to-one, then D has property (n).

To complete the proof of the theorem, we suppose that $x \to x^n$ is not one-to-one and we show that D does not have property (n). Hence, there are distinct elements $a, b \in K$ such that $a^n = b^n$. There is an element ξ of L such that $v_1(\xi - a)$ and $v_2(\xi - b)$ are positive. We write $\xi = a + m_1 = b + m_2$, where $m_i \in M_i$. If t is any element of D, and if $t = c + m$, where $c \in K$ and $m \in M_1 \cap M_2$, $\xi - t\xi^n \equiv a + ca^n \ (M_1)$ and $\xi - t\xi^n \equiv b + cb^n \ (M_2)$. Since $a + ca^n - b - cb^n = a - b \neq 0$, and because $M_1 \cap K = M_2 \cap K = (0)$, it then follows that $\xi - t\xi^n \notin D$ for any $t \in D$, so that D does not have property (n).

The prime field π_2 with two elements has the property that $x \to x^n$ is one-to-one for any positive integer n. Hence, if $D = \pi_2 + (M_1 \cap M_2)$, where M_1 is the maximal ideal of $V_1 = (\pi_2[X])_{(X)} = \pi_2 + M_1$ and, where M_2 is the maximal ideal of $V_2 = (\pi_2[X])_{(X+1)} = \pi_2 + M_2$, we obtain another example of a domain having property (n) for each positive integer, but which is not integrally closed, and hence is not Prüfer.

Fields with the property that $x \to x^n$ is one-to-one for each positive integer n are classified by Theorem 7.2.

THEOREM 7.2. *The field K is such that the mapping $x \to x^n$ of K into K is one-to-one for each positive integer n if and only if K has characteristic two and the prime field of K is algebraically closed in K.*

Proof. Since $1^2 = (-1)^2$, if $x \to x^2$ is one-to-one, K must have characteristic 2. Further, if θ is an element of K algebraic over π_2, then $\pi_2(\theta) = GF(2^n)$ for some positive integer n. In particular, $(\theta)^{2^n-1} = 1 = (1)^{2^n-1}$ so that $\theta = 1$ if $x \to x^{2^n-1}$ is one-to-one. It follows that if $x \to x^n$ is one-to-one for each positive integer n, then π_2 is algebraically closed in K. To prove the converse, consider $\xi_1, \xi_2 \in K$ such that $\xi_1^r = \xi_2^r$ for some positive integer r. If either of ξ_1 or ξ_2 is zero, so is the other. If $\xi_1 \neq 0 \neq \xi_2$, then ξ_1/ξ_2 is a nonzero element of K algebraic over $\pi_2 : (\xi_1/\xi_2)^r = 1$. Hence $\xi_1/\xi_2 = 1$, and $\xi_1 = \xi_2$.

Added in Proof. In connection with the results in §6, James W. Brewer has recently obtained necessary and sufficient conditions in order that a field k should have property (n), for arbitrary n, with respect to any finite algebraic extension field $k(t)$ of k, Brewer's results appear in a paper entitled *Ohm's property* (n) *for field extensions* which he has submitted for publication.

https://doi.org/10.4153/CJM-1968-095-2 Published online by Cambridge University Press

References

1. N. Bourbaki, *Algèbre commutative*, Vol. XXXI, chapitre 7 (Hermann, Paris, 1965).
2. H. S. Butts and W. W. Smith, *Prüfer rings*, Math. Z. *95* (1967), 196–211.
3. R. Gilmer, *Contracted ideals with respect to integral extensions*, Duke Math. J. *34* (1967), 561–572.
4. ——— *The cancellation law for ideals in a commutative ring*, Can. J. Math. *17* (1965), 281–287.
5. ——— *Integral domains which are almost Dedekind*, Proc. Amer. Math. Soc. *15* (1964), 813–818.
6. R. Gilmer and W. Heinzer, *Primary ideals and valuation ideals*. II, Trans. Amer. Math. Soc. *131* (1968), 149–162.
7. R. Gilmer and J. Ohm, *Primary ideals and valuation ideals*, Trans. Amer. Math. Soc. *117* (1965), 237–250.
8. C. U. Jensen, *On characterizations of Prüfer rings*, Math. Scand. *13* (1963), 90–98.
9. W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche*, Math. Z. *41* (1936), 545–577.
10. ——— *Idealtheorie* (Springer, Berlin, 1935).
11. ——— *Zur Theorie der kommutativen Integritätsbereiche*, J. Reine Angew. Math. *192* (1954), 230–252.
12. N. Nakano, *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkörper*, J. Sci. Hiroshima Univ. Ser. A-I Math. *16* (1953), 425–439.
13. J. Ohm, *Integral closure and* $(x, y)^n = (x^n, y^n)$, Monatsh. Math. *71* (1967), 32–39.
14. H. Prüfer, *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, J. Reine Angew. Math. *168* (1932), 1-36.
15. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I (Van Nostrand, Princeton, 1958).
16. ——— *Commutative algebra*, Vol. II (Van Nostrand, Princeton, 1960).

Florida State University,
Tallahassee, Florida

https://doi.org/10.4153/CJM-1968-095-2 Published online by Cambridge University Press