JOURNAL OF ALGEBRA 81, 150–164 (1983)

Finitely Generated Ideals of the Ring of Integer-Valued Polynomials

ROBERT GILMER*

Department of Mathematics and Computer Science, Florida State University, Tallahassee, Florida 32306

AND

WILLIAM W. SMITH†

Department of Mathematics, University of North Carolina, Chapel Hill, North Carolina 27514

Communicated by J. Dieudonné

Received February 5, 1982

1. INTRODUCTION

Throughout this paper, Z denoes the integers, Q the rational numbers, and D the collection of polynomials over Q having the property that $f(a) \in Z$ for every a in Z. After first being studied by Polya [21] and Skolem [23], the domain D has been the subject of several more recent papers [2–14, 16, 17]. In particular, Brizolis established in [4] that D is a Prüfer domain with each finitely generated ideal I determined by the values at integers of the polynomials in I. Specifically, he showed that if $I = (f_1(t),\dots,f_k(t))D$, then $g(t) \in I$ if and only if $g(a) \in (f_1(a),\dots,f_k(a))Z$ for every $a \in Z$. In this paper we continue the study of the finitely generated ideals of D. While our initial efforts were directed toward answering a question of Brizolis [4] as to whether or not each finitely generated ideal of D can be gnerated by two elements, in time we became interested in giving a more explicit description of finite generating sets for ideals of D. Our methods are constructive, and we feel that we have had some success in accomplising this goal.

Section 2 contains some basic results about the arithmetic of D. These results are more number-theoretic than algebraic in nature. In Sections 3 and

* Partial support received from NSF Grant MCS 7903123 during the writing of this paper.
† This work was done at Florida State University while on leave from the University of North Carolina at Chapel Hill.

0021-8693/83 $3.00

4, finite generating sets for ideals of D are discussed and constructed. The main result is an affirmative answer to the question of Brizolis mentioned in the preceding paragraph. Section 5 contains an analysis of the sequences $\{a_n\}_{n=0}^{\infty}$ which are given by an ideal $I = (f_1(t),..., f_k(t))$, in the sense that $a_n = \gcd\{f_1(n),..., f_k(n)\}$ for each n. The characterization of the sequences leads to an alternate argument that each finitely generated ideal can be generated by two elements.

2. Basic Results

This section gives some basic properties of D which are used in later sections. If I is an ideal of D and a is an integer, then $I(a) = \{f(a) \mid f(t) \in I\}$. It follows that $I(a)$ is an ideal of integers and if I is a finitely generated ideal generated by $f_1(t),..., f_k(t)$, then $I(a)$ is generated by the greatest common divisor of $f_1(a),..., f_k(a)$. For each positive integer n, let

$$B_n(t) = \frac{t(t-1)\cdots(t-(n-1))}{n!}$$

and set $B_0(t) = 1$. For a positive integer a, $B_n(a)$ is the familiar binomial coefficient $\binom{a}{n}$. Polya established the following statement as the first basic result about D.

THEOREM 2.1 [21]. *The polynomials $B_n(t)$, for $n \geqslant 0$, form a basis for D as a free abelian group.*

Using the fact that $B_n(k) = 0$ for $0 \leqslant k \leqslant n$ and $B_n(n) = 1$, one obtains the following slightly more general property, which we occasionally use.

THEOREM 2.2. *Given $q_0, q_1,..., q_n$ in Q, there exist unique $r_0, r_1,..., r_n$ in Q such that $f(k) = q_k$ for $0 \leqslant k \leqslant n$, where $f(t) = r_0 B_0(t) + \cdots + r_n B_n(t)$. Moreover, if $q_0,..., q_n$ are in Z, then $r_0,..., r_n$ are in Z.*

The ideal-theoretic properties of D are best summarized with the following theorem of Brizolis.

THEOREM 2.3 [4]. *D is a two-dimensional Prüfer domain.*

Brizolis [4] also established, for finitely generated ideals I and J, that $I = J$ if and only if $I(a) = J(a)$ for every $a \in Z$. We provide in Proposition 2.6 an alternate proof of this result (which also uses Theorem 2.3). We remark that Proposition 2.6 shows that $I = J$ if $I(a) = J(a)$ for all except a finite number of positive integers; this form of the criterion is often more convenient to apply.

PROPOSITION 2.4. *If $F(t)$ and $G(t)$ are in D and $F(a) \in (G(a))Z$ for all except a finite number of positive integers, then $F(t) \in (G(t))D$.*

Proof. Let $\eta(t) = F(t)/G(t) = f(t)/g(t)$, where $f(t)$ and $g(t)$ are in $Z[t]$. Since $g(t)$ has only finitely many zeros, the hypothesis translates to the property $\eta(a) = f(a)/g(a)$ is an integer for all except a finite number of positive integers a. If b is the leading coefficient of g, then the division algorithm in $Z[t]$ can be applied to $b^k f(t)$, $g(t)$ for k sufficiently large. Choose such a k and write $b^k f(t) = g(t)\, q(t) + r(t)$, where $q(t)$, $r(t)$ are in $Z[t]$ and where either $r(t) = 0$ or $\deg r(t) < \deg g(t)$. Then $b^k \eta(t) = q(t) + \eta_1(t)$, where $\eta_1(t) = r(t)/\eta(t)$. Since $\eta_1(a) = b^k \eta(a) - q(a)$, we have $\eta_1(a)$ is an integer for all except a finite number of positive integers. Since either $r(t) = 0$ or $\deg r(t) < \deg g(t)$, we know $\lim_{a \to \infty} \eta_1(a) = 0$. Since $\eta_1(a)$ is an integer for all except a finite number of positive integers, we must have $\eta_1(a) = 0$, and hence $r(a) = 0$ for all except a finite number of positive integers. Therefore $r(t) = 0$, giving $b^k f(t) = g(t)\, q(t)$ and $\eta(t)$ is in $Q[t]$. Now $\eta(a) \notin Z$ implies b^k does not divide $q(a)$. But $q(x)$ in $Z[x]$ implies $q(a + rb^k) \equiv q(a) (\text{Mod } b^k)$ for every integer r. Therefore if there exists one value of a for which b^k does not divide $q(a)$, then there are infinitely many. Since $\eta(a)$ is in Z for all except a finite number of a, we must have $b^k \mid q(a)$ for all a. Therefore $\eta(t)$ is in D and $F(t)$ is in $(G(t))D$.

Proposition 2.4 is closely related to conditions considered by Gunji and McQuillan in [16]. In particular, Proposition 1 of [16] is the case of Proposition 2.4 where the hypothesis on $F(t)$ and $G(t)$ (taken to be in $Z[t]$ in [16], but this is no restriction) is that $F(a) \in (G(a))Z$ for all but a finite number of integers. We note that the proof of Proposition 2.4 shows that its conclusion remains valid if the hypothesis is weakened to the assumption that $F(a) \in G(a)Z$ for infinitely many integers a.

PROPOSITION 2.5. *If I is an invertible ideal of D and $f(t)$ in D has the property that $f(a) \in I(a)$ for all except a finite number of positive integers, then $f(t) \in I$.*

Proof. Choose $G(t)$ to be a nonzero element of I and write $(G(t))D = IJ$, where J is also invertible. For each $h(t)$ in J and for each a for which $f(a) \in I(a)$, we have $f(a)\, h(a) \in I(a)\, J(a) \subseteq (G(a))Z$. By Proposition 2.4, $f(t)\, h(t) \in (G(t))D$. Since this is true for each $h(t)$ in J, we have $f(t)J \subseteq IJ$. Then J invertible implies that $f(t) \in I$.

PROPOSITION 2.6. *If I and J are finitely generated ideals of D, then $I = J$ if and only if $I(a) = J(a)$ for all except a finite number of positive integers a.*

(It then follows that $I(a) = J(a)$ for every integer a.)

Proof. Since D is Prüfer, I and J are invertible and the result follows from Proposition 2.5.

In the sections that follow, we frequently consider the collection of integral values of a polynomial $f(t)$ in D. As Proposition 2.4 indicates, it is often sufficient to consider the sequence $\{f(a)\}_{a=0}^{\infty}$. On occasion we consider the residues of such a sequence modulo p^m for some prime integer p. Here we establish some terminology and a basic result regarding $B_n(t)$. We note for a given positive integer m and for $f(t)$ in D that the collection of integers $J = \{x \mid f(a) \equiv f(a+x) \pmod{m} \text{ for every } a \text{ in } Z\}$ is an ideal of Z. In Proposition 5.1 we show that J is nonzero; hence J is generated by its least positive integer s. We say in this case that $f(t)$ is *periodic* modulo m with *period* s and we write $\pi_m(f) = s$. In order to restrict our considerations to nonnegative integers, we need to know that the integer s is determined by the values of f at positive integers. To wit, it is enough to observe that the set $J_1 = \{x \geqslant 0 \mid f(a) \equiv f(a+x) \pmod{m} \text{ for every } a \geqslant 0\}$ is the set of nonnegative multiples of s; this is an easy exercise and its verification is omitted. The next two results establish the periodicity of $f(t)$ in D modulo p^m, where p is a prime number; periodicity modulo k for each $k > 1$ follows immediately from these two results.

Throughout the proof of Proposition 2.7 and in subsequent discussions we make free use of the "Pascal's Triangle" identity $B_n(a) = B_{n-1}(a-1) + B_n(a-1)$ for $n > 1$ and $a \geqslant 1$. We note that since $B_n(t)$ is a polynomial with rational coefficients, the preceding equality for infinitely many integers a implies, in fact, the polynomial identity $B_n(t) = B_{n-1}(t-1) + B_n(t-1)$.

PROPOSITION 2.7. *Let n, m, and p be positive integers with p a prime. Let v be the integer satisfying $p^v \leqslant n < p^{v+1}$. Then $\pi_{p^m}(B_n) = p^{m+v}$.*

Proof. The proof (by induction) is divided into the following steps.

Step 1. $B_n(p^{m+v}) \equiv 0 \pmod{p^m}$.

$$B_n(p^{m+v}) = \left(\frac{p^{m+v}}{n}\right)\left(\frac{p^{m+v}-1}{1}\right)\cdots\left(\frac{p^{m+v}-(n-1)}{n-1}\right).$$

If $1 \leqslant d \leqslant n-1$ and $p^s \mid\mid d$, then $p^s < n$ so $p^s \mid p^{m+v}$. Therefore $p^s \mid\mid d$ if and only if $p^s \mid\mid (p^{m+v} - d)$. As a result, whether or not $B_n(p^{m+v})$ is congruent to zero modulo p^m is determined by the factor p^{m+v}/n. But $p^r \mid n$ implies $r \leqslant v$, leaving the numerator with a factor of at least p^m. Therefore $B_n(p^{m+v}) \equiv 0 \pmod{p^m}$, completing Step 1.

Step 2 (Induction setup). If $n = 1$, then $v = 0$ the result holds, for it is clear that $B_1(t) = t$ has period p^m modulo p^m. Assume that $B_1, \ldots, B_{n-1}$ satisfy the conclusion of the theorem.

Step 3. $\pi_{p^m}(B_n) = p^t$ for some t satisfying $v+1 \leqslant t \leqslant m+n$. We first show that $B_n(a + p^{m+v}) \equiv B_n(a) \pmod{p^m}$ for every a. It then follows that $\pi_{p^m}(B_n) = p^t$ for some t, where $p^t \mid p^{m+v}$. Since $B_n(0) = B_n(1) = \cdots =$

$B_n(p^v) = \cdots = B_n(n-1) = 0$ and $B_n(n) = 1$, it follows that the period p^t is greater than p^v. This produces the desired inequality $v + 1 \leqslant t \leqslant m + n$. The congruence $B_n(a + p^{m+v}) \equiv B_n(a)$ (Mod p^m) was established for $a = 0$ in Step 1; the general congruence is easily established by an inductive argument (on a) using $B_n(a + p^{m+v}) = B_{n-1}((a-1) + p^{m+v}) + B_n((a-1) + p^{m+v})$. Note that the induction step uses the assumption on B_{n-1} given in Step 2. This completes Step 3.

Step 4. $\pi_{p^m}(B_n) \nmid p^{m+v-1}$, and hence $\pi_{p^m}(B_n) = p^{m+v}$. To establish this we observe that $\pi_{p^m}(B_n) \mid p^{m+v-1}$ implies each of $B_n(p^{m+v-1})$, $B_n(p^{m+v-1} + 1), \ldots, B_n(p^{m+v-1} + (n-1))$ is congruent to zero modulo p^m since $B_n(0) = B_n(1) = \cdots = B_n(n-1) = 0$. These, in turn, produce the following n congruences:

$$B_{n-1}(p^{m+v-1} - 1) + B_n(p^{m+v-1} - 1) \equiv B_n(p^{m+v-1}) \equiv 0 \pmod{p^m},$$

$$B_{n-1}(p^{m+v-1}) + B_n(p^{m+v-1}) \equiv B_n(p^{m+v-1} + 1) \equiv 0 \pmod{p^m},$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$B_{n-1}(p^{m+v-1} + (n-2)) + B_n(p^{m+v-1} + (n-2)) \equiv B_n(p^{m+v-1} + (n-1)) \equiv 0 \pmod{p^m}.$$

It then follows that $B_{n-1}(p^{m+v-1})$, $B_{n-1}(p^{m+v-1} + 1), \ldots, B_{n-1}(p^{m+v-1} + (n-2))$ are also all congruent to zero modulo p^m. Continuing this argument after $n - p^v$ steps we get $B_{p^v}(p^{m+v-1}) \equiv 0$ (Mod p^m). But $B_{p^v}(p^{m+v-1}) = \binom{p^{m+v-1}}{p^v}$, which is known to be exactly divisible by p^{m-1} [19, p. 78]. This contradiction completes Step 4.

THEOREM 2.8. *If $f(t) = a_0 + a_1 B_1(t) + \cdots + a_n B_n(t)$, where each a_i is an integer (hence $f(t) \in D$), then $\pi_{p^m}(f) = p^k$ for some $k \leqslant n + m$.*

Proof. Since $\pi_{p^m}(B_i) \mid p^{n+m}$ for all $i \leqslant n$ by Proposition 2.7, this result easily follows; the congruence $f(a + p^{n+m}) \equiv f(a)$ (Mod p^m) holds for every integer a because it holds for each B_i.

Giving two examples of these last two results, we have $\pi_4(B_7) = 2^4 = 16$. Starting with $B_7(0)$ the sequence of residues modulo 4 is 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 3,... with the given portion repeating. If $f(t) = B_1(t) + 2B_3(t) = t + [t(t-1)(t-2)/3]$, then $\pi_4(f) = 2^2 = 4$, with the sequence of residues being 0, 1, 2, 1, 0, 1, 2, 1,....

3. THE CASE $I \cap Z \neq (0)$.

A commutative unitary ring R is said to have the *n-generator property* if each invertible ideal of R admits a generating set of n elements. For a Prüfer domain R, the n-generator property is equivalent to the condition that each finitely generated ideal of R can be generated by n elements. For many years the question of whether each Prüfer domain has the two-generator property was open. In the positive direction, Heitmann in [18] proved that a d-dimensional Prüfer domain has the $(d+1)$-generator property, but Schülting in [22] gave an example of a two-dimensional Prüfer domain that does not have the two-generator property. Brizolis in [4] raises the question of whether the domain D of integer-valued polynomials has the two-generator property. Since D is two-dimensional, Heitmann's result implies that D has the three-generator property. In the next section we prove that D has the two-generator property. The argument involves a reduction to the case where $I \cap Z = nZ \neq (0)$. We treat this special case separately in this section. The sequence of arguments follows the progression of n being first a prime, then a power of a prime, and finally, an arbitrary $n \neq 0$.

THEOREM 3.1. *Each finitely generated ideal of D containing a prime integer p is generated by two elements, one of which can be taken to be p. Equivalently, D/pD is a Bezout ring for each prime integer p.*

Proof. It suffices to show that for f and g in D, the ideal $I = (p, f, g)$ is of the form (p, h) for some h in D. We consider two cases:

Case 1: $p = 2$. We set $J = (2, f^2 + fg + g^2)$ and show that $I = J$ by showing that $I(a) = J(a)$ for each a in Z. There are three subcases to consider. If $2 \mid f(a)$ and $2 \mid g(a)$, then $I(a) = J(a) = (2)$. If 2 divides one of $f(a)$ or $g(a)$ and not the other, then $I(a) = J(a) = (1)$. If 2 divides neither $f(a)$ nor $g(a)$, then $f(a) \equiv g(a) \equiv 1 \pmod 2$ and hence $f^2(a) + f(a)g(a) + g^2(a) \equiv 1 \pmod 2$, which yields $I(a) = J(a) = (1)$. Therefore, $f^2 + fg + g^2$ is an acceptable choice for h when $p = 2$.

Case 2: $p > 2$. In this case we show for $h = f^{p-1} + g^{p-1}$ and $J = (p, h)$ that $I(a) = J(a)$ for every a in Z. As in the first case, $I(a) = J(a) = (p)$ if p divides both $f(a)$ and $g(a)$. If p does not divide at least one of the two, we have $f^{p-1}(a) + g^{p-1}(a) \equiv 1$ or $2 \pmod p$. Since $p \neq 2$, it follows that $J(a) = (1) = I(a)$.

We remark that the two cases given in this argument can be combined by observing that for any prime p, $GF(p)[X, Y]$ contains a polynomial $h(X, Y)$ with only the origin as a zero in $GF(p) \times GF(p)$. The same result holds over any finite field $GF(p^n)$. For $p = 2$, the polynomial $X^{p(p^n-1)} + (XY)^{p^n-1} + Y^{p(p^n-1)}$ works, while $X^{p^n-1} + Y^{p^n-1}$ works for $p > 2$.

LEMMA 3.2. *Assume that p is a prime integer and s is a positive integer. There exists an element $H(t)$ in D such that $H(b) \equiv 0 \pmod p$ if $p^s \| b$, while $H(b) \not\equiv 0 \pmod p$ if $p^{s+1} \mid b$.*

Proof. First we consider $B_{p^s}(t)$. If $p^s \mid\mid b$ and if $b = p^s c$, then

$$B_{p^s}(b) = \binom{p^s c}{p^s}\binom{p^s c - 1}{1} \cdots \binom{p^s c - (p^s - 1)}{p^s - 1},$$

and from this representation we see that the exact power of p that divides the denominator term d, for $1 \leqslant d \leqslant p^s - 1$, is the same as the exact power p that divides the numerator term $p^s c - d$. Since $p \nmid c$, it follows that $B_{p^s}(b) \not\equiv 0$ (Mod p) in this case. Similar reasoning shows that if $p^{s+1} \mid b$, then $B_{p^s}(b) \equiv 0$ (Mod p). An $H(t)$ satisfying the conclusion of Lemma 3.2 can be taken to be $H(t) = [B_{p^s}(t) - 1][B_{p^s}(t) - 2] \cdots [B_{p^s}(t) - (p-1)]$.

THEOREM 3.3. *If I is a finitely generated ideal of D such that $I \cap Z = p^k Z$, where p is a prime and $k \geqslant 1$, then I can be generated by two elements, one of which can be taken to be p^k.*

Proof. We use induction on k, the case $k = 1$ being covered in Theorem 3.1. Assume the result for $k \leqslant s$ and let I be a finitely generated ideal such that $I \cap Z = p^{s+1}Z$. Set $B = pD + I$. Since D is a Prüfer domain, we have $I = B(I\colon B)$, where $I\colon B = B^{-1}I = I\colon (p)$; thus, $I\colon B$ is a finitely generated ideal and it contains p^s, but not p^{s-1}. Now B is a finitely generated ideal which contains p, so the induction hypothesis applied to $I\colon B$ and B yields f and g in D such that $B = (p, g)$ and $I\colon B = (p^s, f)$. We choose an element $H(t)$ of D as in Lemma 3.2 and observe that $H(f(t))$ is also in D. (In fact, the definition of D implies that D is closed under composition of functions.) We now set $h(t) = pf(t) + g^2(t)f(t) + p^s g(t)\, H(f(t))$ and $C = (p^{s+1}, h)$. $I = B(I\colon B) = (p, g)(p^s, f) = (p^{s+1}, p^s g, g, pf, fg)$. We prove that $I = C$ by showing that $I(a) = C(a)$ for each a in Z. The following chart indicates the various cases to be considered. It is routine to verify, using the properties of $H(t)$, that the indicated common value of $I(a)$ and $C(a)$ is obtained.

Case	$I(a)$ and $C(a)$
$p \nmid g(a)$ and $p \nmid f(a)$	(1)
$p \nmid g(a)$ and $p^v \mid\mid f(a)$, $v < s$	(p^v)
$p \nmid g(a)$ and $p^s \mid\mid f(a)$	(p^s)
$p \nmid g(a)$ and $p^{s+1} \mid\mid f(a)$	(p^s)
$p \nmid g(a)$ and $p^v \mid f(a)$, $v > s + 1$	(p^s)
$p \mid g(a)$ and $p \nmid f(a)$	(p)
$p \mid g(a)$ and $p^v \mid\mid f(a)$, $v < s$	(p^{s+1})
$p \mid g(a)$ and $p^s \mid\mid f(a)$	(p^{s+1})
$p \mid g(a)$ and $p^{s+1} \mid\mid f(a)$	(p^{s+1})
$p \mid g(a)$ and $p^v \mid f(a)$, $v > s$	(p^{s+1})

It is helpful to keep in mind in computing $I(a)$ that $I(a) = B(a) \cdot (I\colon B)(a)$ since the two terms in the factorization are more easily computed. Thus, I is generated by two elements, one of which is p^{s+1}.

To complete the general case $I \cap Z = nZ \neq (0)$, we need the following result, which is valid for any commutative ring. We include its brief proof for the sake of completeness.

LEMMA 3.4. *Assume that* $A = (a, f_1, \dots, f_n)$ *and* $B = (b, g_1, \dots, g_n)$ *are ideals of the commutative ring* R *with identity, where* $(a, b) = R$. *Then* AB *can be generated by* $n+1$ *elements, one of which can be chosen to be* ab.

Proof. Choose r and s in R such that $ar + bs = 1$ and set $C = (ab, arg_1 + bsf_1, \dots, arg_n + bsf_n)$. We shown that $C = AB$; the inclusion $C \subseteq AB$ is clear. For the reverse inclusion, we note that for each i we have

$$ag_i = a(arg_i + bsf_i) + (g_i - f_i)\, sab,$$

$$bf_i = b(arg_i + bsf_i) + (f_i - g_i)\, rab,$$

$$f_i\, g_j = rf_i ag_j + sg_j bf_i.$$

Now AB is generated by elements of the form ab, ag_j, bf_j, $f_i\, g_j$. Those of the first three types are in C by the first two equations. Knowing that ag_j and bf_i are in C implies that $f_i\, g_j$ is in C by the third equation.

THEOREM 3.5. *If* I *is a finitely generated ideal of* D *such that* $I \cap Z = nZ \neq (0)$, *then* n *can be chosen as one of a set of two generators for* I.

Proof. Assume that n has r distinct prime factors. We use induction on r. The case $r = 0$ is trivial, and Theorem 3.3 established the case $r = 1$. We assume the result for $1 \leqslant r \leqslant t$ and consider $n = p_1^{e_1} \cdots p_{t+1}^{e_{t+1}}$. Let $B = I + (p_{t+1}^{e_{t+1}})$ and write $I = BC$, where $C = I\colon B = I\colon (p_{t+1}^{e_{t+1}})$. It follows that $C \cap Z = p_1^{e_1} \cdots p_t^{e_t} Z$ and $B \cap Z = p_{t+1}^{e_{t+1}} Z$. By the induction hypothesis, there exist f and g in D such that $B = (p_{t+1}^{e_{t+1}}, f)$ and $C = (p_1^{e_1} \cdots p_t^{e_t}, g)$. Lemma 3.4 shows that $I = BC = (n, h)$, where

$$h = rp_{t+1}^{e_{t+1}} g + sp_1^{e_1} \cdots p_t^{e_t} f,$$

with r and s being integers such that $rp_{t+1}^{e_{t+1}} + sp_1^{e_1} \cdots p_t^{e_t} = 1$.

One comment on the results of this section is appropriate at this point. Theorem 3.1 establishes that D/pD is a Bezout domain. This fact follows immediately from the primary result stated in Theorem 3.1 since the finitely generated proper ideals of D/pD are of the form I/pD, where I is a finitely generated ideal of D for which $I \cap Z = pZ$. Hence, by the argument given in Theorem 3.1, $I = (p, f)$ for some f in D. In the general case, however, for a proper ideal I/nD of D/nD, it only follows that $I \cap Z$ *contains* nZ.

Theorem 3.5 gives n to be one of two generators of I only for the case $I \cap Z = nZ$. It is true, however, that D/nD is Bezout, a result which is established in Section 5 of this paper. To illustrate this remark with an example, consider the ideal $I = (2, t, t(t-1)/2)$. We have shown that this ideal can be generated by two elements, one of which can be chosen to be 2. In fact, our arguments are constructive and yield $I = (2, t^2 + t^2(t-1)/2 + t^2(t-1)^2/4)$. We note that $I(a) = (2)$ if $a \equiv 0$ (Mod 4) and $I(a) = (1)$ if $a \equiv 1, 2$, or 3 (Mod 4). In considering the ideal $I/4D$ in $D/4D$, however, our techniques yield no element f such that $I = (4, f)$. Results of Section 5 will show that, in fact, $I = (4, [B_2(t)]^2 + [B_2(t+1)]^2 + [B_2(t+2)]^2)$.

4. The Case $I \cap Z = (0)$.

In the first part of this section, we extend Theorem 3.5 to the case where I is a finitely generated ideal of D with $I \cap Z = (0)$. Following the primary result that such ideals are generated by two elements, we give some additional observations on ideals of this type.

THEOREM 4.1. *If I is a finitely generated ideal of D with $I \cap Z = (0)$, then I can be generated by two elements.*

Proof. Assume that $I \neq (0)$. Then $I \cap Z = (0)$ implies that $IQ[t]$ is a proper ideal of the principal ideal domain $Q[t]$. Therefore there exists a nonzero element $f(t)$ of $I \cap Z[t]$ such that $IQ[t] = f(t)\,Q[t]$. Since D is a Prüfer domain, $(f(t))D = IB$ for some finitely generated ideal B of D. We have $(f(t))Q[t] = (IQ[t])(BQ[t]) = (f(t)Q[t])(BQ[t])$, so $BQ[t] = Q[t]$, which implies $B \cap Z \neq (0)$. Therefore B, and B^{-1}, can be generated by two elements by Theorem 3.5. It follows that $I = (f(t))\,B^{-1}$ can be generated by two elements.

We now combine Theorems 3.5 and 4.1 for the general statement.

THEOREM 4.2. *The Prüfer domain D has the two-generator property.*

The next result involves taking a closer look at the proof of Theorem 4.1, resulting in a more explicit description of the form the two generators take for various ideals.

PROPOSITION 4.3. *If $I = (n, f(t))$, where $n \neq 0$ and $f(t) \in D$, then there exists $g(t) \in D$ such that $I^{-1} = (1, g(t)/n)$. If J is a finitely generated ideal with $J \cap Z = (0)$, then there exist $f(t)$ and $g(t)$ in D and $n \neq 0$ in Z such that $J = (f(t), f(t)\,g(t)/n)$.*

Proof. The second statement follows from the argument given in Theorem 4.1 and the first statement since $J = (f(t))I^{-1}$, where $f(t) \in D$ and I

is an ideal with $I \cap R \neq (0)$. To prove the first statement, let B be the ideal of D such that $(n)D = IB$. Then B is finitely generated with $n \in B$; in fact, $B = nI^{-1}$. We know $B = (n, g(t))$ for some $g(t)$ in D, from which it follows that $I^{-1} = (1, g(t)/n)$.

The remaining results of this section address several questions concerning the ideals of Z, D, and $Q[t]$ and their various extensions and contractions. We first mention a simple example that illustrates some of the results. We know from elementary number theory that $t((t^{p-1} - 1)/p)$ is in D, where p is a prime number. Observing that $(t^{p-1} - 1)/p$ is in $Q[t]$ but not in D, we see that $tD \subsetneq tQ[t] \cap D$ and that tD is not a prime ideal of D (invertible prime ideals of Prüfer domains are maximal [15, p. 289]). Since $(t, t(t^{p-1} - 1)/p)\, D \subseteq tQ[t] \cap D$, we see that $tQ[t] \cap D$ properly contains an infinite set of distinct ideals, each of which exends to $tQ[t]$. That this situation always occurs and that, in fact, the ideal $tQ[t] \cap D$ is not finitely generated is given in the next result.

PROPOSITION 4.4. *If $f(t) \in D$ with $(f(t))D \cap Z = (0)$ (that is, $f(t)$ is not a constant polynomial), then $(f(t))D$ is properly contained in the ideal $I = f(t)Q[t] \cap D$. Moreover, I is not finitely generated.*

Proof. Obviously, the result is established if we show that I is not finitely generated. If I is finitely generated, there exist $n \neq 0$ such that $nI \subseteq (f(t))D$ (see, for example, the proof of Theorem 4.1). In particular, this says that if $R(t) \in Q[t]$ is such that $f(t)R(t)$ is in D, then $nf(t)R(t) = f(t)h(t)$ for some $h(t)$ in D. It then follows that $nR(t) = h(t)$ is in D. We exhibit an $R(t)$ which contradicts this. We know that the congruence $f(t) \equiv 0 \pmod p$ has a solution for infinitely many primes p. Choose a prime p such that $p > n$ and $p \mid f(a)$ for some a in Z. Consider $B_p(f(t))$, which is in D since D is closed under composition. Then $B_p(f(t)) = f(t)[(f(t) - 1) \cdots (f(t) - p + 1)/p!]$, so if $R(t)$ is the second factor in this product, we have $B_p(f(t)) = f(t)R(t)$ is in $f(t)Q[t] \cap D = I$. On the other hand, $nR(t)$ is not in D since $nR(a)$ is not in Z because $p \nmid n$ and $p \nmid (f(a) - d)$ for any d, $1 \leqslant d \leqslant p - 1$.

In the same spirit we note that for any prime integer p, we have $t(t^{p-1} - 1)$ is in pD since $t(t^{p-1} - 1)/p$ is in D. Neither t nor $t^{p-1} - 1$ is in pD so pD is not a prime ideal. Of course, we already knew this since it is not maximal in the Prüfer domain D. However, pD is a radical ideal of D, a fact we observe in the more general context of Proposition 4.5.

PROPOSITION 4.5. *if I is a finitely generated ideal of D and if $I(a)$ is a radical ideal of Z for each a in Z, then I is a radical ideal of D.*

Proof. Suppose $f(t)$ is in D with $f^k(t)$ in I for some positive integer k. Then $f^k(a)$ is in $I(a)$ for each a in Z. Since $I(a)$ is assumed to be a radical ideal of Z, we have $f(a) \in I(a)$ for each a in Z. This implies that $f(t) \in I$.

PROPOSITION 4.6. *If I is a finitely generated ideal of D such that $I \cap Z$ is a nonzero radical ideal of Z, then I is a radical ideal of D.*

Proof. We know by the assumption $I \cap Z$ is a nonzero radical ideal of Z that I contains a square-free positive integer n. Therefore $n \in I(a)$ for every a, and hence $I(a)$ is a radical ideal for each a. By Proposition 4.5, I is a radical ideal of D.

THEOREM 4.7. *For an integer $n > 1$, D/nD is von Neumann regular if and only if n is square-free.*

Proof. If n is not square-free, then $nD \cap Z = nZ$ is not a radical ideal of Z. It follows that D/nD is not reduced, and hence D/nD is not von Neumann regular. If n is square-free, then $I \cap Z$ is a radical ideal of Z for each finitely generated ideal I containing nD. Thus each finitely generated ideal of D/nD is a radical ideal, and D/nD is von Neumann regular [1, p. 46; 15, p. 111].

5. THE IDEALS $I(a)$

In this section we study the sequence of ideals $I(a)$, $a = 0, 1, 2, \ldots$, obtained from a finitely generated ideal I of D for which $I \cap Z \neq (0)$. In the course of characterizing these sequences, we obtain a proof, different from the one given in Section 3, that each ideal of this type is generated by two elements. The stronger result mentioned earlier, that D/nD is Bezout, is obtained in Theorem 5.6.

Section 2 contains some results concerning the periodicity of the sequences $f(a)$ modulo a power of a prime. Our first results in this section continue that development.

PROPOSITION 5.1. *Assume that n is a positive integer with prime factorization $p_1^{e_1} \cdots p_k^{e_k}$. If $f(t) \in D$, then f is periodic modulo n and $\pi_n(f)$ is a positive integer of the form $p_1^{h_1} \cdots p_k^{h_k}$, where $h_i \geqslant 0$ for each i.*

Proof. Theorem 2.8 states that there exists $h_i \geqslant 0$ such that $\pi_{p_i^{e_i}}(f) = p_i^{h_i}$ for each i. Since $f(a + p_1^{h_1} \cdots p_k^{h_k}) \equiv f(a)$ (Mod $p_i^{e_i}$) for each i, it follows that $f(a + p_1^{h_1} \cdots p_k^{h_k}) \equiv f(a)$ (Mod n). On the other hand, if $\pi_n(f) = m$, then $f(a + m) \equiv f(a)$ (Mod n) for each a, which implies that $f(a + m) \equiv f(a)$ (Mod $p_i^{e_i}$) for each i. Since $\pi_{p_i^{e_i}}(f) = p_i^{h_i}$, it follows that $p_i^{h_i} \mid m$ for each i. Therefore $\pi_n(f) = p_1^{h_1} \cdots p_k^{h_k}$. Specifically, the above argument shows that $\pi_{rs}(f) = \pi_r(f)\, \pi_s(f)$ whenever $(r, s) = 1$.

PROPOSITION 5.2. *If I is a finitely generated ideal of D and $n \geqslant 1$, then the sequence $\{I(a) + nZ\}_{a=0}^{\infty}$ of ideals of Z is periodic with period of the form $p_1^{h_1} \cdots p_k^{h_k}$, where $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n.*

Proof. Let $I=(f_1,...,f_m)$. By Proposition 5.1, each f_i is periodic modulo n and $\pi_n(f_i)$ is of the form $p_1^{g_1}\cdots p_k^{g_k}$. But $f_i(a)\equiv f_i(b)$ (Mod n) implies $(n,f_i(a))=(n,f_i(b))$. Taking u to be the least common multiple of the $\pi_n(f_j)$, $1\leqslant j\leqslant m$, we have u is of the form $p_1^{r_1}\cdots p_k^{r_k}$. Moreover, for any x, $f_i(a+ux)\equiv f_i(a)$ (Mod n), for $1\leqslant i\leqslant m$, implies $(f_1(a),...,f_m(a),n)=(f_1(a+ux),...,f_n(a+ux),n)$. Since $I(a)+nZ=(f_1(a),...,f_m(a),n)$ for every a, we have $I(a)+nZ=I(a+ux)+nZ$ for every a and every x. Thus $\{I(a)+nZ\}_{a=0}^{\infty}$ is periodic with period a divisor of u. Any divisor of u must be of the form required in the statement of the result.

We observe at this point that $n\in I$ in the above gives $I(a)+nZ=I(a)$. Looking at the same example given at the end of Section 3, $I=(4,t,t(t-1)/2)$, we have $I(a)=(2)$ if $a\equiv 0$ (Mod 4) and $I(a)=(1)$ if $a\equiv 1,2,$ or 3 (Mod 4). The problem of producing a single $f(t)\in D$ such that $I=(4,f(t))$ reduces to that of producing a polynomial $f(t)$ in D such that $f(i)\equiv a_i$ (Mod 4), where $\{a_i\}$ represents the sequence 2, 1, 1, 1, 2, 1, 1, 1,.... Such an f will yield the desired result since, as in the above argument, $(4,f(i))=(4,a_i)=(a_i)$ for every i. Hence $(4,f(t))(a)=I(a)$ for every $a\geqslant 0$ and it follows that $(4,f(t))=I$. The polynomial $4+B_3^2(t)+B_3^2(t+1)+B_3^2(t+2)$ is such an element of D. The next two results show for sequences of the form $\{I(a)+nZ\}_{a=0}^{\infty}$ how to construct such a function. We first consider the case $n=p^m$.

PROPOSITION 5.3. *Let $\{a_i\}_{i=0}^{\infty}$ be a sequence whose residues modulo p^m are periodic with period p^k. There exists $f(t)$ in D such that $f(i)\equiv a_i$ (Mod p^m) for every $i\geqslant 0$.*

Proof. We let $\varepsilon_j=\{\varepsilon_{ji}\}_{i=0}^{\infty}$ denote the unique periodic sequence with period p^k which has all of its first p^k values zero except for the jth value, which is 1. For example,

$$\varepsilon_0=\{[1,0,0,...,0],[1,0,0,...,0],...\},$$

$$\varepsilon_1=\{[0,1,0,...,0],[0,1,0,...,0],...\},$$

$$\vdots$$

$$\varepsilon_{p^k-1}=\{[0,0,...,1],[0,0,...,1],...\}.$$

The [ ] are used to emphasize the repeating blocks of p^k numbers. If we construct $F_j(t)$ in D such that $F_j(i)\equiv\varepsilon_{ji}$ (Mod p^m) for each i and j, then it is clear that $f(t)=a_0F_0(t)+\cdots+a_{p^k-1}F_{p^k-1}(t)$ will satisfy the conclusion of Proposition 5.3. Moreover, if $F_{p^k-1}(t)$ has been constructed, then we can take $F_{p^k-a}(t)$ to be $F_{p^k-1}(t+a-1)$. Since D is closed under composition, F_{p^k-a} is in D. We have thus reduced the problem to constructing $F(t)$ in D such that $F(i)\equiv 0$ (Mod p^m) for $0\leqslant i<p^k-1$, $F(p^k-1)\equiv 1$ (Mod p^m), and $F(a)$ periodic modulo p^m with period p^k. We claim that $F(t)=[B_{p^k-1}(t)]^{p^{m-1}(p-1)}$

is such a function. The significance of the exponent $v = p^{m-1}(p-1)$ is that $W^v = 1$ for each unit W in $Z/(p^m)$ and $W^v = 0$ for each nonunit W in $Z/(p^m)$. By Proposition 2.7, $\pi_p(B_{p^k-1}) = p^k$ so $B_{p^k-1}(a) \equiv B_{p^k-1}(b)$ (Mod p) whenever $a \equiv b$ (Mod p^k). Since $B_{p^k-1}(i) = 0$ for $0 \leqslant i < p^k - 1$ and since $B_{p^k-1}(p^k - 1) = 1$, it follows that $B_{p^k-1}(a)$ is a nonunit of $Z/(p^m)$ for $a \equiv 0, 1, ..., p^k - 2$ (Mod p^k) and $B_{p^k-1}(a)$ is a unit of $Z/(p^m)$ for $a \equiv p^k - 1$ (Mod p^k). Therefore, $F(a) \equiv 0$ (Mod p^m) if $a \equiv 0, 1, ..., p^k - 2$ (Mod p^k) and $F(a) \equiv 1$ (Mod p^m) if $a \equiv p^k - 1$ (Mod p^k). Thus, F has the properties needed to construct the desired f as outlined at the beginning of the proof.

In reviewing the example initially given at the end of Section 3 and mentioned again immediately before Proposition 5.3, one can see an example of the construction technique used in the proof of Proposition 5.3.

PROPOSITION 5.4. *Assume $n > 1$ is an integer with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$. Let $\{a_i\}_{i=0}^{\infty}$ be a sequence of integers such that modulo $p_j^{e_j}$, the sequence $\{a_i\}_{i=0}^{\infty}$ is periodic with period a power of p_j for each j between 1 and k. Then there exists an $f(t)$ in D such that $f(i) \equiv a_i$ (Mod n) for each $i \geqslant 0$.*

Proof. For $1 \leqslant j \leqslant k$, let $s_j = n/p_j^{e_j}$. Then $(s_1, ..., s_k) = 1$ and there exist integers $u_1, ..., u_k$ so that $u_1 s_1 + \cdots + u_k s_k = 1$. By Proposition 5.3, there exist $f_1, ..., f_k$ in D such that $f_j(i) \equiv a_i$ (Mod $p_j^{e_j}$) for each $i \geqslant 0$ and $1 \leqslant j \leqslant k$. Let $f = \sum_{j=1}^{k} u_j s_j f_j$. We show that f satisfies the required conditions. For a given r between 1 and k, $p_r^{e_r}$ divides each s_j except s_r. Hence for each r between 1 and k, $f(i) = \sum_{j=1}^{k} u_j s_j f_j(i) \equiv u_r s_r f_r(i) \equiv u_r s_r a_i$ (Mod p^{e_r}). Thus, $f(i) - a_i \equiv a_i(u_r s_r - 1) \equiv a_i(-\sum_{j \neq r} u_j s_j) \equiv 0$ (Mod $p_r^{e_r}$). It follows that $f(i) - a_i \equiv 0$ (Mod n) for each $i \geqslant 0$, which completes the proof.

Before summarizing the results of this section with a theorem characterizing ideal sequences $\{I(a)\}_{a=0}^{\infty}$ we introduce some terminology. If $\{C_i\}_{i=0}^{\infty}$ is a sequence of ideals of Z, then we say the sequence is *periodic modulo m of period k* if the sequence of ideals $\{\phi(C_i)\}_{i=0}^{\infty}$ is periodic of period k in Z/mZ, where ϕ denotes the canonical homomorphism from Z to Z/mZ. An equivalent form of the definition is to say that the sequence $\{C_i + mZ\}_{i=0}^{\infty}$ is a periodic sequence of ideals in Z of period k. One must be careful in considering the period of a sequence of ideals modulo m not to confuse the periodicity with that of the original generators before passing to Z/mZ. We give the following example, pointing out its relationship to the problem being considered here. Let $\{A_i\}$ be the sequence of ideals in Z given by $6Z$, Z, $2Z$, $3Z$, $2Z$, Z,..., periodic with the indicated period six. This sequence is also periodic modulo 3 and modulo 2 as follows:

Modulo 3: looking at $A_i + 3Z$, we have the sequence $3Z$, Z, Z, $3Z$, Z, Z,... of period 3. Notice that the original generators of the A_i, when reduced modulo 3, produce a periodic sequence, but not of period 3.

Modulo 2: looking at $A_i + 2Z$ we have the sequence $2Z, Z, 2Z, Z, \ldots$ of period 2. We note that the original sequence A_i is given by $A_i = I(i)$, where $I = (6, t^2)$. A characterization of the sequences $\{I(a)\}_{a=0}^{\infty}$, for I a finitely generated ideal of D for which $I \cap Z \neq (0)$, is contained in the next result.

THEOREM 5.5. *Assume that n is a positive integer with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$.*

(1) *If $\{A_i\}_{i=0}^{\infty}$ is a sequence of ideals of Z such that $\bigcap_{i=0}^{\infty} A_i \supseteq nZ$ and if for each j between 1 and k, the sequence $\{A_i\}_{i=0}^{\infty}$ is periodic modulo $p_j^{e_j}$ of period a power of p_j, then $\{A_i\}_{i=0}^{\infty}$ is of the form $\{I(i)\}_{i=0}^{\infty}$ for some finitely generated ideal I of D containing n. Moreover, I is of the form $(n, h(t))$ for some $h(t)$ in D.*

(2) *Conversely, if J is a finitely generated ideal of D such that $J \cap Z \supseteq nZ$, then the sequence $\{J(i)\}_{i=0}^{\infty}$ is periodic modulo $p_j^{e_j}$ with period a power of p_j for each j between 1 and k.*

Proof. For each j, let $B_{ji} = A_i + p_j^{e_j}Z$ and let $B_{ji} = b_{ji}Z$ with $b_{ji} > 0$. Then for each j, our assumption is that the sequence $\{b_{ji}\}_{i=0}^{\infty}$ is periodic modulo $p_j^{e_j}$ with period a power of p_j. By Proposition 5.3, there exist $f_j(t)$ in D such that $f_j(i) \equiv b_{ji}$ (Mod $p_j^{e_j}$). This implies that $(p_j^{e_j}, f_j(i)) = b_{ji}$ for each i. In other words, the ideal $I_j = (p_j^{e_j}, f_j(t))$ produces the sequence of ideals B_{ji}. Letting $I = I_1 \cdots I_k$, we first observe that $I(i) = I_1(i)\, I_2(i) \cdots I_k(i) = B_{1i} B_{2i} \cdots B_{ki} = A_i$ since the p_j are distinct primes and since $n = p_1^{e_1} \cdots p_k^{e_k}$ is in A_i. On the other hand, by Lemma 3.4 in Section 3, $I = (n, h(t)$ for a suitably chosen $h(t) \in D$. This last comment verifies the last statement of (1). (2) is simply a restatement of Proposition 5.2, with the added assumption $n \in J$ implying $n \in I(a)$ for each a, and hence $I(a) + nZ = I(a)$.

THEOREM 5.6. *For each positive integer n, D/nD is a Bezout ring.*

Proof. We observe that in Theorem 5.5, if I is a finitely generated ideal of D containing n, then $I(i)$ contains n for each i, so n can be chosen to be one of two generators for I. Therefore I/nD is principal.

We conclude with some remarks concerning the restriction in this paper to finitely generated ideals of D. While this restriction is unnecessary in a few of the paper's results, the more substantial theorems all use Proposition 2.7, and that result is false without the hypothesis of finite generation. In fact, Brizolis in [2, 4] determines the maximal ideals of D lying over a given prime pZ of Z as follows. Let $\hat{Z}_p$ be the p-adic completion of Z. For $\alpha \in \hat{Z}_p$, the ideal $M_{\alpha,p} = \{f \in D \mid f(\alpha) \in p\hat{Z}_p\}$ is maximal in D and lies over pZ; moreover, $\{M_{\alpha,p} \mid \alpha \in \hat{Z}_p\}$ is the set of all maximal ideals of D lying over pZ, and $M_{\alpha,p}$ and $M_{\beta,p}$ are distinct for $\alpha \neq \beta$. Finally, Brizolis in [4] shows that if $\alpha \notin Z$, then $M_{\alpha,p}(a) = Z$ for each integer a. Hence $1 \in M_{\alpha,p}(a)$ for each a, but $1 \notin M_{\alpha,p}$.

REFERENCES

1. N. BOURBAKI, "Commutaive Algebra," Addison–Wesley, Reading, Mass., 1972.
2. D. BRIZOLIS, Hilbert rings of integral-valued polynomials, *Comm. Algebra* **3** (1975), 1051–1081.
3. D. BRIZOLIS, Ideals in rings of integer-valued polynomials, *J. Reine Angew. Math.* **285** (1976), 28–52.
4. D. BRIZOLIS, A theorem on ideals in Prüfer rings of integral-valued polynomials, *Comm. Algebra* **7** (1979), 1065–1077.
5. D. BRIZOLIS AND E. G. STRAUS, A basis for the ring of doubly integer-valued polynomials, *J. Reine Angew. Math.* **286/287** (1976), 187–195.
6. P. J. CAHEN, Polynomes à valeurs entières, *Canad. J. Math.* **24** (1972), 747–754.
7. P. J. CAHEN, Fractions rationelles à valeurs entières, *Ann. Sci. Univ. Clermont Ser. Math.* **16** (1978), 85–100.
8. P. J. CAHEN AND J.-L. CHABERT, Coefficient et valeurs d'un polynome, *Bull. Sci. Math.* **95** (1971), 295–304.
9. J.-L. CHABERT, Anneaux de "polynomes à valeurs entières et anneaux de Fatou," *Bull. Soc. Math. France* **99** (1971), 273–283.
10. J.-L. CHABERT, Anneaux de polynomes à valeurs entières, *Colloque Algèbre Rennes* 1972.
11. J.-L. CHABERT, Les idéaux premières de l'anneau des polynomes à valeurs entières, *J. Reine Angew. Math.* **293/294** (1977), 275–283.
12. J.-L. CHABERT, Polynomes à valeurs entières at propriété de Skolem, *J. Reine Angew. Math.* **303** (1978), 366–378.
13. J.-L. CHABERT, Anneaux de Skolem, *Arch. Math. (Basel)* **32** (1979), 555–568.
14. J.-L. CHABERT, Polynomes à valeurs entières ainsi que leurs dérivées, *Ann. Sci. Univ. Clermont Ser. Math.* **18** (1979), 47–64.
15. R. GILMER, "Multiplicative Ideal Theory," Dekker, New York, 1972.
16. H. GUNJI AND D. L. MCQUILLAN, On rings with a certain divisibility property, *Michigan Math. J.* **22** (1975), 289–299.
17. H. GUNJI AND D. L. MCQUILLAN, Polynomials with integral values, *Proc. Roy. Irish Acad. Sect. A* **78** (1978), 1–7.
18. R. C. HEITMANN, Generating ideals in Prüfer domains, *Pacific J. Math.* **62** (1976), 117–126.
19. I. N. HERSTEIN, "Topics in Algebra," Blaisdell, Waltham, Mass., 1964.
20. M. D. LARSEN AND P. J. MCCARTHY, "Multiplicative Theory of Ideals," Academic Press, New York, 1971.
21. G. POLYA, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919), 97–116.
22. H.-W. SCHÜLTING, Über die Erzeugendenanzahl invertierbarer Ideale in Prüferringen, *Comm. Algebra* **7** (1979), 1331–1349.
23. TH. SKOLEM, Ein Satz über ganzwertige Polynome, *Norske Vid. Selsk. (Trondheim)* **9** (1936), 111–113.